Trend Micro Apex One™

Service Pack 1 Patch 1

インストールガイド

※注意事項

複数年契約について

・お客さまが複数年契約（複数年分のサポート費用前払い）された場合でも、各製品のサポート期間については、当該契約期間によらず、製品ごとに設定されたサポート提供期間が適用されます。

・複数年契約は、当該契約期間中の製品のサポート提供を保証するものではなく、また製品のサポート提供期間が終了した場合のバージョンアップを保証するものではありませんのでご注意ください。

・各製品のサポート提供期間は以下の Web サイトからご確認いただけます。

https://success.trendmicro.com/jp/solution/000207383

法人向け製品のサポートについて

・法人向け製品のサポートの一部または全部の内容、範囲または条件は、トレンドマイクロの裁量により随時変更される場合があります。

・法人向け製品のサポートの提供におけるトレンドマイクロの義務は、法人向け製品サポートに関する合理的な努力を行うことに限られるものとします。

商標について

TRENDMICRO、TREND MICRO、ウイルスバスター、InterScan、INTERSCAN VIRUSWALL、InterScanWebManager、InterScan Web Security Suite、PortalProtect、Trend Micro Control Manager、Trend Micro MobileSecurity、VSAPI、Trend Park、Trend Labs、Network VirusWall Enforcer、Trend Micro USB Security、InterScan Web Security Virtual Appliance、InterScan Messaging Security Virtual Appliance、Trend Micro Reliable Security License、TRSL、Trend Micro Smart Protection Network、SPN、SMARTSCAN、Trend Micro Kids Safety、Trend Micro Web Security、Trend Micro Portable Security、Trend Micro Standard Web Security、Trend Micro Hosted Email Security、Trend Micro Deep Security、ウイルスバスタークラウド、スマートスキャン、Trend Micro Enterprise Security for Gateways、Enterprise Security for Gateways、Smart Protection Server、Deep Security、ウイルスバスター ビジネスセキュリティサービス、SafeSync、Trend Micro NAS Security、Trend Micro Data Loss Prevention、Trend Micro オンラインスキャン、Trend Micro Deep Security Anti Virus for VDI、Trend Micro Deep Security Virtual Patch、SECURE CLOUD、Trend Micro VDI オプション、おまかせ不正請求クリーンナップサービス、Deep Discovery、TCSE、おまかせインストール・バージョンアップ、Trend Micro Safe Lock、Deep Discovery Inspector、Trend Micro Mobile App Reputation、Jewelry Box、InterScan Messaging Security Suite Plus、おもいでバックアップサービス、おまかせ！スマホお探しサポート、保険&デジタルライフサポート、おまかせ！迷惑ソフトクリーンナップサービス、InterScan Web Security as a Service、Client/Server Suite Premium、Cloud Edge、Trend Micro Remote Manager、Threat Defense Expert、Next Generation Threat Defense、Trend Micro Smart Home Network、Retro Scan、is702、デジタルライフサポートプレミアム、Air サポート、Connected Threat Defense、ライトクリーナー、Trend Micro Policy Manager、フォルダシールド、トレンドマイクロ認定プロフェッショナルトレーニング、Trend Micro Certified Professional、TMCP、XGen、InterScan Messaging Security、InterScan Web Security、Trend Micro Policy-based Security Orchestration、Writing Style DNA、Securing Your Connected World、Apex One、Apex Central、MSPL、TMOL、TSSL、ZERO DAY INITIATIVE、Edge Fire、Smart Check、Trend Micro XDR、Trend Micro Managed XDR、OT Defense Console、Edge IPS、Trend Micro Cloud One、スマスキャ、Cloud One、Cloud One - Workload Security、Cloud One - Conformity、ウイルスバスター チェック！、Trend Micro Security Master、Trend Micro Service One、

P/N: APEM09525/220511_JP (2023/01)

プライバシーと個人データの収集に関する規定

トレンドマイクロ製品の一部の機能は、お客さまの製品の利用状況や検出にかかわる情報を収集してトレンドマイクロに送信します。この情報は一定の管轄区域内および特定の法令等において個人データとみなされることがあります。トレンドマイクロによるこのデータの収集を停止するには、お客さまが関連機能を無効にする必要があります。

Trend Micro Apex One により収集されるデータの種類と各機能によるデータの収集を無効にする手順については、次の Web サイトを参照してください。

https://www.go-tm.jp/data-collection-disclosure

重要

データ収集の無効化やデータの削除により、製品、サービス、または機能の利用に影響が発生する場合があります。Trend Micro Apex One における無効化の影響をご確認の上、無効化はお客さまの責任で行っていただくようお願いいたします。

トレンドマイクロは、次の Web サイトに規定されたトレンドマイクロのプライバシーポリシー (Global Privacy Notice) に従って、お客さまのデータを取り扱います。

https://www.trendmicro.com/ja_jp/about/legal/privacy-policy-product.html

目次

第 3 章：Trend Micro Apex One のバージョンアップ

第 6 章：トラブルシューティングのリソース

第 7 章：テクニカルサポート

付録 A：導入例

索引

はじめに

はじめに

Trend Micro Apex One インストールガイドへようこそ。本書では、Apex One サーバのインストール要件と手順、およびサーバとセキュリティエージェントのバージョンアップ方法について説明します。

この章は次のトピックで構成されます。

注意

セキュリティエージェントのインストールについては、管理者ガイドを参照してください。

Apex One 付属のドキュメント

Apex One のドキュメントには、次のものが含まれます。

表 1. Apex One 付属のドキュメント

ドキュメント	説明
インストールガイド	Apex One サーバをインストールし、サーバとエージェントをバージョンアップするための要件および手順を説明した PDF ドキュメント 注意 マイナーリリースバージョン、Service Pack、または Patch にはインストールガイドが付属していない場合があります。
システム要件	Apex One サーバをインストールし、サーバとエージェントをバージョンアップするためのシステムの最小要件と推奨要件を説明した PDF ドキュメント
管理者ガイド	使用開始にあたっての情報、セキュリティエージェントのインストール手順、および Apex One サーバとエージェントの管理について説明した PDF ドキュメント
ヘルプ	操作手順、使用にあたってのアドバイス、および目的別の作業手順を提供する、WebHelp または CHM 形式のオンラインヘルプ。Apex One サーバ、エージェントコンソール、および Apex One のインストーラからアクセスできます。
Readme ファイル	既知の問題のリストと基本的なインストール手順が含まれています。ヘルプや関連ガイドには含まれない最新の製品情報も含まれる場合があります。
Apex One サポートページ	本 Web サイトでは、「よくあるお問い合わせ」、「製品 Q&A」、「サポートセンターへの問い合わせ」などの役立つ情報をご紹介していますのでご活用ください。 http://tmqa.jp/corp14-banner1

最新のドキュメントおよび Readme ファイルは、次の Web サイトからダウンロードできます。

http://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

対象読者

Apex One 付属のドキュメントは、次のユーザを対象としています。

- Apex One 管理者: Apex One サーバおよびセキュリティエージェントのインストールと管理を含む Apex One 管理の責任者。ネットワーキングおよびサーバ管理についての高度な知識を持つユーザであることが想定されています。
- エージェントユーザ: エンドポイントにセキュリティエージェントをインストールしているユーザ。エンドポイントのスキルレベルは限定されず、コンピュータ初心者から上級ユーザまでを対象とします。

ドキュメントの表記規則

このドキュメントでは、次の表記規則を使用しています。

表 2. ドキュメントの表記規則

表記	説明
 注意	設定上の注意
 ヒント	推奨事項
 重要	必須の設定や初期設定、および製品の制限事項に関する情報
 警告!	避けるべき操作や設定についての注意

用語

次の表は、Apex One 付属のドキュメントで使用されている正式な用語を示しています。

表 3. Apex One の用語

用語	説明
セキュリティエージェント	Apex One エージェントプログラム
エージェントエンドポイント	セキュリティエージェントがインストールされているエンドポイント
エージェントユーザ (またはユーザ)	エージェントエンドポイントでセキュリティエージェントを使用するユーザ
サーバ	Apex One サーバプログラム
サーバコンピュータ	Apex One サーバがインストールされているエンドポイント
管理者 (または Apex One 管理者)	Apex One サーバの管理者
コンソール	Apex One サーバおよびエージェントを設定および管理するためのユーザインタフェース。 Apex One サーバプログラム用のコンソールを「Web コンソール」、セキュリティエージェントプログラム用のコンソールを「セキュリティエージェントコンソール」と呼びます。
セキュリティリスク	ウイルス/不正プログラム、スパイウェア/グレーウェア、および Web からの脅威の総称
製品サービス	ウイルス対策、ダメージクリーンナップサービス、Web レピュテーションおよびスパイウェア対策を含みます。これらはすべて Apex One サーバのインストール時にアクティベートされます。
Apex One サービス	Microsoft 管理コンソール (MMC) によってホストされるサービス。たとえば、Apex One Master Service の `ofcservice.exe` などです。

用語	説明
プログラム	セキュリティエージェントやプラグインマネージャも含まれます。
コンポーネント	セキュリティ上の脅威の検索、検出、および処理を実行するものです。
エージェントインストールフォルダ	セキュリティエージェントのファイルが含まれるエンドポイント上のフォルダ。インストール時の初期設定では、インストールフォルダは次のいずれかの場所になります。 C:¥Program Files¥Trend Micro¥Security Agent C:¥Program Files (x86)¥Trend Micro¥Security Agent
サーバインストールフォルダ	Apex One サーバのファイルが含まれるエンドポイント上のフォルダ。インストール時の初期設定では、インストールフォルダは次のいずれかの場所になります。 C:¥Program Files¥Trend Micro¥Apex One C:¥Program Files (x86)¥Trend Micro¥Apex One たとえば、サーバのインストールフォルダで¥PCCSRV の下にあるファイルのフルパスは次のようになります。 C:¥Program Files¥Trend Micro¥Apex One¥PCCSRV¥<ファイル名>
スマートスキャンエージェント	スマートスキャンを使用するように設定されているセキュリティエージェント
従来型スキャンエージェント	従来型スキャンを使用するように設定されているセキュリティエージェント

用語	説明
デュアルスタック	IPv4 アドレスと IPv6 アドレスの両方を持つエンティティ。 例: • IPv4 アドレスと IPv6 アドレスの両方を持つエンドポイント • デュアルスタックエンドポイントにインストールされたセキュリティエージェント • エージェントにアップデートを配信するアップデートエージェント • IPv4 アドレスと IPv6 アドレスを変換できる、DeleGate などのデュアルスタックプロキシサーバ
IPv4 シングルスタック	IPv4 アドレスのみを持つエンティティ
IPv6 シングルスタック	IPv6 アドレスのみを持つエンティティ
プラグインソリューション	プラグインマネージャから配信される、Apex One に本来備わる機能およびプラグインプログラム

第 1 章

Apex One のインストールとバージョンアップの計画

この章では、Trend Micro Apex One™のインストールとバージョンアップに際しての準備や注意事項について説明します。

重要

- Apex Central と Apex One サーバの同一 OS へのインストールは サポートされていません。

  詳細については、https://success.trendmicro.com/jp/solution/000286643 を参照してください。

この章で説明する内容には、次の項目が含まれます。

Apex One サーバの要件

次の項目では、Apex One サーバのインストールまたはバージョンアップを実行する前の注意事項について説明します。

- 20 ページの「OS のサポート」
- 21 ページの「SQL Server の要件」
- 22 ページの「セキュリティエージェントのサポート」
- 23 ページの「インストールの確認」

OS のサポート

次の表は、Apex One サーバでの OS のサポートと移行の可否を簡単にまとめたものです。

ヒント

トレンドマイクロでは、Apex One サーバのインストールやバージョンアップの前に、対象のサーバコンピュータで Windows Update を実行しておくことをお勧めします。

OS	Apex One	Apex One Service Pack 1
Windows Server 2012	○	○
Windows Server 2012 R2	○	○
Windows Server 2016	○	○
Windows Server 2019	○	○
Windows Server 2022	-	○

重要

Apex One では、Apache サーバのサポートが完全に廃止されています。

SQL Server の要件

Apex One では、前のバージョンのウイルスバスター Corp.で使用されていた旧型の CodeBase データベースモデルのサポートは廃止されています。インストール前に独自の SQL Server を用意するか、サーバインストールプロセス中に Apex One セットアッププログラムで SQL Server 2016 SP1 Express をインストールすることができます。

重要

Apex One へのバージョンアップ後、Apex One Web コンソール上には、旧型の CodeBase データベースのバックアップに使用されていた古い [データベースバックアップ] 画面は表示されなくなります。

次の表は、Apex One サーバでのデータベースのサポートと移行の可否を簡単にまとめたものです。

データベース	APEX ONE	ENDPOINT SENSOR 利用時
CodeBase	-	-
SQL Server 2008 Express SP2	○	-
SQL Server 2008	○	-
SQL Server 2008 R2	○	-
SQL Server 2012	○	-
SQL Server 2014	○	-
SQL Server 2016	○	-
SQL Server 2016 SP1	○	○
SQL Server 2016 Express SP1	○	-
SQL Server 2017	○	○

注意

Apex One のインストールやバージョンアップ時に Endpoint Sensor 機能もインストールする場合は、インストールプロセスを開始する前に、サポート対象のバージョンの SQL Server で [検索のためのフルテキスト抽出とセマンティック抽出] を有効にする必要があります。

Endpoint Sensor の要件の詳細については、29 ページの「Apex One Endpoint Sensor」を参照してください。

セキュリティエージェントのサポート

次の表は、セキュリティエージェントの要件と推奨設定の概要を示しています。

重要

エンドポイントで多数のアプリケーションが同時に実行されている場合は、リソースの一時的な高負荷が発生する可能性があります。対象エンドポイントですでにメモリまたはディスク容量が不足している場合は、Apex One セキュリティエージェントのインストールまたはバージョンアップの前に必要なハードウェアコンポーネントをバージョンアップすることをお勧めします。

広範囲にわたる検索処理中に、十分なパフォーマンスを確保できるよう、記載されているシステムの最小要件をセキュリティエージェントプログラム専用のリソースとして割り当てることをお勧めします。

項目	説明
HTTPS のサポート	Apex One サーバとセキュリティエージェントの間では HTTPS 通信が必要になります。 **重要** バージョンアップ時に HTTPS 通信を許可しない場合、Apex One Service Pack 1 サーバへのバージョンアップは行えません。

項目	説明
サーバ/エージェント間通信	トレンドマイクロでは、インストール完了後の [グローバルエージェント設定] 画面で、Apex One サーバとセキュリティエージェントの間の通信に対する AES-256 暗号化を有効にすることをお勧めします。
OS のサポート	Apex One では、特定の Windows OS を実行しているエンドポイントのみがサポートされています。 Apex One サーバとセキュリティエージェントの要件の一覧については、次の Web サイトを参照してください。http://www.go-tm.jp/corp/req バージョンアップ中に、セットアッププログラムによって、サーバへのレポートを行うすべてのエンドポイントがサポート対象の OS を実行しているかどうかが確認されます。サポートされていない OS が検出された場合は、バージョンアップを続行できません。 Apex One サーバへのバージョンアップ前に、サポートされていない OS にインストールされているすべてのエージェントを別のウイルスバスター Corp.サーバに移動するか、エージェントプログラムをアンインストールしてください。

インストールの確認

次の表は、Apex One サーバとセキュリティエージェントのインストールが正常に完了しているかどうかを確認する方法の概要を示しています。

項目	説明
Apex One サーバ	以下のサービスが実行されていることを確認します。 • Apex One Master Service (`OfcService.exe`) • Apex One Plug-in Manager (`OfcAoSMgr.exe`) • Apex One Active Directory Service (`OSCEIntegrationService.exe`) • Apex One Log Receiver Service (`OfcLogReceiverSvc.exe`) • Apex One Deep Discovery Service (`ofcDdaSvr.exe`) • Apex One database process (`DbServer.exe`)

セキュリティエージェント	以下のサービスが実行されていることを確認します。
	• デスクトッププラットフォームの場合:
	  • Apex One Common Client Solution Framework Service (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT RealTime Scan (`Ntrtscan.exe`)
	  • Apex One NT Firewall (`Tmpfw.exe`)
	  • Trend Micro Unauthorized Change Prevention Service (`TMBMSRV.exe`)
	• サーバプラットフォームの場合:
	  • Apex One Common Client Solution Framework Service (`TmCCSF.exe`)
	  • Apex One NT Listener (`Tmlisten.exe`)
	  • Apex One NT RealTime Scan (`Ntrtscan.exe`)

Apex Central の拡張機能の要件

Apex Central Web コンソールとの統合によって利用できる追加のセキュリティ機能を配信する予定がある場合は、その追加機能に対する Apex One システム要件について理解しておくようにしてください。以下のトピックでは、

システム要件、インストールやバージョンアップの情報、および強化された製品機能に関連する追加情報の概要を説明しています。

Apex One アプリケーションコントロール

注意

Trend Micro Endpoint Application Control は日本国内においては販売しておりません。

表 1-1. 前提条件

項目	要件
システム要件	Apex One サーバおよびセキュリティエージェントの要件に準ずる
ライセンス	Apex One アプリケーションコントロールライセンスは、Trend Micro Apex One 発売と同時に「Client/Server Suite Premium」ライセンスに標準添付となりました。スタンドアロンまたはオプションのライセンスはありません。
Apex Central への登録	ライセンス認証とセキュリティエージェントのポリシーの配信に必要

項目	要件
Trend Micro Endpoint Application Control との互換性	• サーバ: アプリケーションコントロールがインストールされた Apex One サーバは、Trend Micro Endpoint Application Control がインストールされたサーバ上に存在できます (推奨しません)。 重要 Trend Micro Endpoint Application Control サーバ設定には、Apex One アプリケーションコントロール機能との互換性はありません。Apex Central Web コンソールを使用して、すべてのポリシーを手動で設定する必要があります。 • エージェント: アプリケーションコントロールポリシーを Apex One セキュリティエージェントに配信すると、セキュリティエージェントは自動的に既存の Trend Micro Endpoint Application Control エージェントをアンインストールしてから、Apex One アプリケーションコントロール設定を適用します。

表 1-2. 新規インストール情報

種類	説明
サーバ	Apex One セットアッププログラムでは、Apex One サーバの標準インストール時にアプリケーションコントロール機能が自動的にインストールされます。 アクティベーションコードの対象にアプリケーションコントロールが含まれていることが確認されると、Apex One は、Trend Micro Application Control Service を Apex One サーバコンピュータ上で開始します。

種類	説明
エージェント	セキュリティエージェントプログラムには Application Control Service が含まれていますが、セキュリティエージェントの標準インストール時に、ただちにインストールされることはありません。Apex One アプリケーションコントロール機能をセキュリティエージェントにインストールするには、Apex Central Web コンソールからアプリケーションコントロールポリシーを有効化および配信する必要があります。 セキュリティエージェントがアプリケーションコントロール設定を受信すると、セキュリティエージェントにアプリケーションコントロール機能がインストールされます。

表 1-3. バージョンアップの注意事項

種類	説明
ウイルスバスター Corp.サーバ	Apex One ライセンスに含まれているアプリケーションコントロールのアクティベーションは、新規インストールのみを対象としています。ウイルスバスター Corp.サーバからバージョンアップする場合は、販売代理店に問い合わせて新規ライセンスを入手し、そのライセンスでアプリケーションコントロール機能をアクティベートする必要があります。 Apex One セットアッププログラムでは、Apex One サーバの標準インストール時に Apex One アプリケーションコントロール機能が自動的にインストールされます。
Trend Micro Endpoint Application Control サーバ	Apex One では、スタンドアロンの Trend Micro Endpoint Application Control サーバから Apex One アプリケーションコントロール機能へのバージョンアップや設定の移行はサポートされていません。 **重要** Trend Micro Endpoint Application Control サーバ設定には、Apex One アプリケーションコントロール機能との互換性はありません。Apex Central Web コンソールを使用して、すべてのポリシーを手動で設定する必要があります。

種類	説明
Trend Micro Endpoint Application Control エージェント	Apex One では、Trend Micro Endpoint Application Control エージェントプログラムから Apex One セキュリティエージェントへのバージョンアップはサポートされていません。 Apex One セキュリティエージェントを Trend Micro Endpoint Application Control エージェントがインストールされたエンドポイントにインストールし、Apex Central コンソールからアプリケーションコントロールポリシーを配信した場合、セキュリティエージェントは自動的に Trend Micro Endpoint Application Control エージェントをアンインストールし、Apex One アプリケーションコントロール機能をインストールします。

表 1-4. インストールの確認

種類	説明
Apex One サーバ	この機能の有効なライセンスを備えた Apex One サーバをインストールした後は、以下を確認できます。 • Trend Micro Application Control Service が Apex One サーバコンピュータで実行されていること。 • Application Control Service フォルダが Apex One サーバコンピュータの以下の場所にあること。 <サーバのインストールフォルダ>/iServiceSvr/iAC • Application Control Service インストールログが Apex One サーバコンピュータの以下の場所にあること。 %windir%/OFCMAS.LOG
セキュリティエージェントエンドポイント	セキュリティエージェントをインストールして Apex Central からアプリケーションコントロールポリシーを配信した後は、以下を確認できます。 • Trend Micro Application Control Service (Agent) がセキュリティエージェントエンドポイントで実行されていること。 • Application Control Service フォルダがエンドポイントの以下の場所にあること。 <セキュリティエージェントのインストールフォルダ>/iService/iAC

表 1-5. インストール後の設定

設定	説明
サーバ	Apex Central Web コンソールで、[運用管理] > [アップデート] > [手動アップデート]の順に移動し、ソフトウェア安全性評価パターンファイルがダウンロードされていることを確認します。
セキュリティエージェントエンドポイント	Apex Central Web コンソールで、[ポリシー] > [ポリシー管理]の順に移動し、Apex One セキュリティエージェントポリシーの [アプリケーションコントロールの設定] を必要に応じて追加または変更します。

Apex One Endpoint Sensor

Apex One™ Endpoint Sensor (以下、Endpoint Sensor) のライセンスを購入し、Apex Central と統合したお客様は、Endpoint Sensor を利用できます。Endpoint Sensor ポリシーの設定は、Apex Central Web コンソールからのみ可能です。

Apex One サーバをインストールする前に、正しいバージョンの SQL Server にアクセスできることを確認してください。Endpoint Sensor 機能を使用する場合は、特定のバージョンの SQL Server をインストールして準備する必要があります。

注意

Endpoint Sensor サービスをインストールしなかった場合や、[検索のためのフルテキスト抽出とセマンティック抽出] が有効になっているサポート対象のバージョンの SQL Server を選択しなかった場合に、Endpoint Sensor を後で使用するには、Windows の [コントロール パネル] にある [プログラムのアンインストールまたは変更] にアクセスする必要があります。

Apex One サーバを選択して、[変更] をクリックします。

- 30 ページの前提条件
- 32 ページの新規インストール情報
- 33 ページのバージョンアップの注意事項

表 1-6. 前提条件

項目	要件
システム要件	サーバ: Apex One サーバの OS 要件に準ずる (SQL Server の要件は異なる) エンドポイント: Apex One セキュリティエージェントのシステム要件に準ずる **重要** この機能が公式にサポートされているのは次のプラットフォームのみです。 • Windows 7 SP1 • Windows 8.1 • Windows 10
ライセンス	• Apex One Endpoint Sensor ライセンス (Apex Central でアクティベート) • 既存の Trend Micro Endpoint Sensor ライセンス (Apex Central でアクティベート)
Apex Central への登録	ライセンス認証とセキュリティエージェントのポリシーの配信に必要

項目	要件

Trend Micro Endpoint Sensor との比較	• スタンドアロンの Trend Micro Endpoint Sensor サーバがインストールされたサーバに、Apex One Endpoint Sensor 機能がインストールされた Apex One サーバを共存させる場合 (推奨しません):
	  • スタンドアロンの Trend Micro Endpoint Sensor サーバを無効にします。
	  • スタンドアロンの Trend Micro Endpoint Sensor のファイルとデータベースは、サーバコンピュータに残るので、パフォーマンスに影響が出る可能性があります。
	
	重要
	スタンドアロンの Trend Micro Endpoint Sensor サーバの設定は、Apex One Endpoint Sensor 機能と互換性がありません。Apex Central Web コンソールを使用して、すべてのポリシーを手動で設定する必要があります。
	• エージェント: Endpoint Sensor ポリシーを Apex One セキュリティエージェントに配信すると、セキュリティエージェントは、Apex One Endpoint Sensor の設定を適用する前に、スタンドアロンの Trend Micro Endpoint Sensor エージェントを自動的にアンインストールします。

Redis サービス	Apex One サーバコンピュータには、既存の Redis サービスをインストールできません。既存の Redis サービスをアンインストールしてから、セットアッププログラムを使用して新しいサービスをインストールする必要があります。 確認 [Endpoint Sensor のインストール] 画面で [次へ] をクリックした後

項目	要件
SQL Server のバージョン	• SQL Server 2017 • SQL Server 2016 SP1 注意 この機能では、SQL Server Express のバージョンはサポートされていません。 確認 [Apex One データベースセットアップ] 画面で [次へ] をクリックした後
データベース設定	[検索のためのフルテキスト抽出とセマンティック抽出] を有効にする [検索のためのフルテキスト抽出とセマンティック抽出] の有効化の詳細については、SQL Server のドキュメントを参照してください。 確認 [Apex One データベースセットアップ] 画面で [次へ] をクリックした後
	データベースメンテナンス機能を使用するための tempdb データベースへのアクセス権 確認 なし

表 1-7. 新規インストール情報

種類	説明
サーバ	Apex One セットアッププログラムでは、Apex One サーバの標準インストール時に、Apex One Endpoint Sensor 機能をインストールするオプションを選択できます。

種類	説明
エージェント	セキュリティエージェントプログラムには Endpoint Sensor サービスが含まれていますが、セキュリティエージェントの標準インストール中にただちにインストールが実行されるわけではありません。セキュリティエージェントに Endpoint Sensor サービスをインストールするには、Apex Central Web コンソールで Endpoint Sensor ポリシーを有効にして配信する必要があります。 セキュリティエージェントが Endpoint Sensor の設定を受信すると、セキュリティエージェントにより Endpoint Sensor サービスがインストールされます。

表 1-8. バージョンアップの注意事項

種類	説明
ウイルスバスター Corp.サーバ	Apex One セットアッププログラムでは、Apex One サーバの標準バージョンアップ時に、Apex One Endpoint Sensor 機能をインストールするオプションを選択できます。
Trend Micro Endpoint Sensor サーバ	Apex One では、スタンドアロンの Trend Micro Endpoint Sensor サーバから Apex One Endpoint Sensor 機能へのバージョンアップや設定の移行はサポートされていません。 **重要** スタンドアロンの Trend Micro Endpoint Sensor サーバの設定は、Apex One Endpoint Sensor 機能と互換性がありません。Apex Central Web コンソールを使用して、すべてのポリシーを手動で設定する必要があります。
Trend Micro Endpoint Sensor エージェント	Apex One では、Trend Micro Endpoint Sensor エージェントプログラムの Apex One セキュリティエージェントへのバージョンアップをサポートしていません。 スタンドアロンの Trend Micro Endpoint Sensor エージェントがインストールされているエンドポイントに Apex One セキュリティエージェントをインストールし、 Apex Central コンソールから Endpoint Sensor ポリシーを配信した場合、セキュリティエージェントにより、Trend Micro Endpoint Sensor エージェントが自動的にアンインストールされ、Apex One Endpoint Sensor 機能がインストールされます。

Managed Detection and Response サービス

Managed Detection and Response (MDR) サービスは、Endpoint Sensor を購入したうえで、MDR サービスを購入し登録した場合のみに利用可能となります。MDR サービスの要件は、次の表に示した追加のタスク要件を除き、Endpoint Sensor の要件に準じます。MDR サービスの購入についていては、トレンドマイクロの営業担当者または販売代理店にお問い合わせください。

タスク	ディスク容量の追加要件
診断タスク	MDR サービスで診断タスクが開始されると、Apex One サーバで追加のログ情報を処理するために、(100 エンドポイントあたり) 20GB のディスク容量が追加で必要になります。
Trend Micro Investigation Kit (TMIK)	MDR サービスによって TMIK が配信されると、Apex One サーバで追加のログ情報を処理するために、(100 エンドポイントあたり) 40GB のディスク容量が追加で必要になります。

Apex One 仮想パッチ

- 34 ページの前提条件
- 35 ページの新規インストール情報
- 36 ページのバージョンアップの注意事項
- 37 ページのインストールの確認
- 37 ページのインストール後の設定

表 1-9. 前提条件

項目	要件
システム要件	Apex One サーバおよびセキュリティエージェントに準ずる
ライセンス	• 仮想パッチライセンス (Trend Micro Virtual Patch for Endpoint) は、「Client/Server Suite Premium」 ライセンスに含まれます • 既存の Trend Micro Virtual Patch for Endpoint ライセンス (Apex Central でアクティベート)

項目	要件
Apex Central への登録	ライセンス認証とセキュリティエージェントのポリシーの配信に必要
Trend Micro Virtual Patch for Endpoint との互換性	• サーバ: 仮想パッチがインストールされている Apex One サーバは、Trend Micro Virtual Patch for Endpoint がインストールされたサーバ上に存在できます (推奨しません)。 • エージェント: 仮想パッチポリシーを Apex One セキュリティエージェントに配信すると、セキュリティエージェントは Apex One 仮想パッチの設定を適用する前に、あらゆる既存の Trend Micro Virtual Patch Agent を自動的にアンインストールします。
他のトレンドマイクロ製品との互換性	次のトレンドマイクロ製品には、Apex One 仮想パッチ機能との互換性がありません。 • Deep Security Agent • 旧脆弱性対策オプションのクライアント 互換性のないエージェントプログラムがインストールされた状態のエンドポイントにセキュリティエージェントをインストールした場合、Apex One 仮想パッチ機能をアクティベートすることはできません。Apex One 仮想パッチ機能をアクティベートする前に、競合プログラムをアンインストールする必要があります。

表 1-10. 新規インストール情報

種類	説明
サーバ	Apex One セットアッププログラムでは、Apex One サーバの標準インストール中に Apex One 仮想パッチ機能がインストールされます。 アクティベーションコードの対象に仮想パッチが含まれていることが確認されると、Apex One により Apex One サーバコンピュータで Trend Micro Vulnerability Protection Service が起動されます。

種類	説明
エージェント	セキュリティエージェントプログラムには Apex One 仮想パッチ機能が含まれていますが、セキュリティエージェントの標準インストール中にただちにインストールが実行されるわけではありません。仮想パッチ機能をセキュリティエージェントにインストールするには、Apex Central Web コンソールから仮想パッチポリシーを有効にして配信する必要があります。 仮想パッチの設定を受信すると、セキュリティエージェントにより仮想パッチ機能がインストールされます。

表 1-11. バージョンアップの注意事項

種類	説明
ウイルスバスター Corp.サーバ	Apex One ライセンスに含まれているのは、新規インストール用の仮想パッチのアクティベーションのみです。ウイルスバスター Corp.サーバからバージョンアップする場合は、仮想パッチ機能をアクティベートするための新しいライセンスの取得について販売代理店にお問い合わせください。 Apex One セットアッププログラムでは、Apex One サーバの標準インストール中に Apex One 仮想パッチ機能がインストールされます。
Trend Micro Virtual Patch Manager	Apex One では、スタンドアロンの Trend Micro Virtual Patch Manager から Apex One 仮想パッチ機能へのバージョンアップや設定の移行をサポートしていません。
Trend Micro Virtual Patch Agent	Apex One では、Trend Micro Virtual Patch Agent プログラムから Apex One セキュリティエージェントへのバージョンアップをサポートしていません。 Trend Micro Virtual Patch Agent がインストールされているエンドポイントに Apex One セキュリティエージェントをインストールして、Apex Central コンソールから仮想パッチポリシーを配信した場合、セキュリティエージェントにより Trend Micro Virtual Patch Agent が自動的にアンインストールされ、Apex One 仮想パッチ機能がインストールされます。

表 1-12. インストールの確認

種類	説明

Apex One サーバ	この機能の有効なライセンスを備えた Apex One サーバをインストールした後は、以下を確認できます。
	• Trend Micro Vulnerability Protection Service が Apex One サーバコンピュータで実行されていること。
	• Vulnerability Protection Service フォルダが Apex One サーバコンピュータの次の場所に存在すること。
	`<サーバのインストールフォルダ>/iServiceSvr/iVP`
	• Vulnerability Protection Service のインストールログが Apex One サーバコンピュータの次の場所に存在すること。
	`<サーバのインストールフォルダ>/iServiceSvr/iVP/install.log`

セキュリティエージェントエンドポイント	セキュリティエージェントをインストールし、Apex Central から仮想パッチポリシーを配信したら、次のことを確認できます。 • Trend Micro Vulnerability Protection Service (Agent) がセキュリティエージェントエンドポイント上で実行されていること。 • Vulnerability Protection Service フォルダが、エンドポイントの次の場所に存在すること。 `<セキュリティエージェントのインストールフォルダ>/iService/iVP`

表 1-13. インストール後の設定

設定	説明
サーバ	Apex Central Web コンソールで、[運用管理] > [アップデート] > [予約アップデート] に移動し、仮想パッチパターンファイルの自動アップデートが予約されていることを確認します。
セキュリティエージェントエンドポイント	Apex Central Web コンソールで、[ポリシー] > [ポリシー管理] に移動し、Apex One セキュリティエージェント ポリシーの [仮想パッチの設定] を必要に応じて追加または編集します。

インストールとバージョンアップのチェックリスト

Apex One サーバのインストールまたはバージョンアップでは、次の情報の入力を求められます。

表 1-14. インストールとバージョンアップのチェックリスト

インストール情報	インストールの種類	
	新規インストール	バージョンアップ
Apex One のインストールパス 初期設定のサーバインストールパスは次のとおりです。 • C:¥Program Files¥Trend Micro¥Apex One • C:¥Program Files (x86)¥Trend Micro¥Apex One (x64 タイプのプラットフォームの場合) インストールパスを指定するか、初期設定のパスを使用します。パスが存在しない場合は、自動的に作成されます。	○	× (バージョンアップ前と同じパスが使用されます)
プロキシサーバ設定 Apex One サーバがプロキシサーバを介してインターネットに接続する場合、次の項目を指定します。 • プロキシタイプ (HTTP または SOCKS 4) • サーバ名/IP アドレス • ポート • プロキシ認証アカウント情報	○	×

インストール情報	インストールの種類	
	新規インストール	バージョンアップ
Web サーバの設定 Web サーバは、Web コンソールの CGI を実行し、エージェントから命令を受け取ります。以下を指定します。 • HTTP ポート: 初期設定のポートは 8080 です。IIS の初期設定の Web サイトを使用している場合は、HTTP サーバの TCP ポートを確認してください。 警告! 多くの企業が HTTP 通信用の初期設定の TCP ポートとしてポート 80 および 8080 を使用しているため、HTTP 経由のハッカーおよびウイルス/不正プログラム攻撃の多くがこれらのポートを使用して行われます。現在これらの初期設定ポート番号を使用している場合は、別のポート番号を使用してください。 セキュリティで保護された接続を有効にしている場合: • SSL 証明書の有効期間 • SSL ポート番号 (初期設定: 4343)	○	×

登録
 	
アクティベーションコードを取得するためにユーザ登録を行ってください。登録には、次の情報が必要です。
 	
• 更新ユーザ:
 	
  • オンライン登録アカウント (ログオン名とパスワード)
 	
• アカウントのないユーザ:
 	
  • レジストレーションキー
	○	○

アクティベーション アクティベーションコードの入手	○	○

インストール情報	インストールの種類	
	新規インストール	バージョンアップ
統合 Smart Protection Server のインストール 統合サーバをインストールする場合は、次の情報を指定します。 • SSL 証明書の有効期間 • SSL ポート	○	○
セキュリティエージェントのインストール	○	×
管理者アカウントのパスワード セットアップでは、Web コンソールのログオン用ルートアカウントが作成されます。以下を指定します。 • ルートアカウントのパスワード セキュリティエージェントの不正なアンインストールやアンロードを防ぐために、次の項目を指定します。 • セキュリティエージェントのアンインストール/アンロード用パスワード	○	×
セキュリティエージェントのインストールパス セキュリティエージェントをインストールするエージェントエンドポイントのディレクトリを指定します。以下を指定します。 • インストールパス: 初期設定のエージェントインストールパスは `C:¥Program Files¥Trend Micro¥Security Agent` または `C:¥Program Files (x86)¥Trend Micro¥Security Agent` です。インストールパスを指定するか、初期設定のパスを使用します。パスが存在しない場合には、インストール時に作成されます。 • セキュリティエージェント通信ポート番号	○	× (バージョンアップ前と同じパスが使用されます)

インストール情報	インストールの種類	
	新規インストール	バージョンアップ
データベースバックアップ ロールバック用に Apex One サーバをバックアップするサーバコンピュータ上の場所を指定します。 注意 バックアップパッケージには少なくとも 300MB の空きディスク容量が必要で、完了までに時間がかかることがあります。	×	○
サーバ認証証明書 Apex One では、インストール時に既存の認証証明書を検出しようと試みます。Apex One で証明書が検出されない場合は、新しい証明書のバックアップパスワードを指定します。	○	○
プログラムフォルダのショートカット Apex One サーバのインストールフォルダへのショートカットは、Windows の [スタート] メニューに表示されます。初期設定のショートカット名は、[Apex One サーバ-<サーバ名>] です。別の名前を指定するか、初期設定の名前を使用します。	○	×

互換性についての既知の問題

ここでは、他社製アプリケーションがインストールされたエンドポイントに Apex One サーバをインストールする際に発生する、互換性の問題について説明します。詳細については、他社製アプリケーションのドキュメントを参照してください。

Microsoft IIS Lockdown ツールおよび URLScan

Microsoft IIS Lockdown ツールまたは URLScan を使用している場合は、次の Apex One ファイルがロックダウンされることにより、セキュリティエージェントとサーバ間の通信がブロックされる可能性があります。

- 設定 (`.ini`) ファイル
- データ (`.dat`) ファイル
- ダイナミックリンクライブラリ (`.dll`) ファイル
- 実行可能 (`.exe`) ファイル

URLScan によるエージェント/サーバ間の通信障害を防ぐには

手順

1. Trend Micro Apex One サーバがインストールされているコンピュータの World Wide Web Publishing サービスを停止します。
2. URLScan の設定ファイルを変更し、上記で指定したファイルの種類を許可します。
3. World Wide Web Publishing サービスを再起動します。

Microsoft Exchange Server

セキュリティエージェントをサーバと同時にインストールする場合、Apex One はエージェントが検索するすべてのファイルにアクセスします。Microsoft Exchange Server ではメッセージがローカルディレクトリのキューに入れられるため、Exchange Server でメッセージを処理できるようにこれらのディレクトリを検索から除外する必要があります。

Apex One は、Microsoft Exchange 2000/2003 のすべてのディレクトリを自動的に検索から除外します。この設定は Web コンソールから設定できます ([エージェント] > [グローバルエージェント設定] > [検索設定] の [セキュリティ設定] タブ)。Microsoft Exchange 2007 の検索除外の詳細については、次の Web サイトを参照してください。

https://technet.microsoft.com/ja-jp/library/bb332342(EXCHG.80).aspx

データベースサーバ

データベースサーバを検索することは可能ですが、データベースにアクセスするアプリケーションのパフォーマンスが低下する可能性があります。データベースとそのバックアップフォルダは、リアルタイム検索の対象から除外することを検討してください。データベースの検索は、業務時間外などの影響が少ない時間帯に手動検索で実行することをお勧めします。

第 2 章

Trend Micro Apex One のインストール

この章では、Trend Micro Apex One のインストール手順について説明します。

この章で説明する内容には、次の項目が含まれます。

新規インストールの注意事項

重要

Apex Central と Apex One サーバの同一 OS へのインストールは サポート されていません。

Apex One サーバの新規インストールを実行する場合には、次の項目を考慮してください。

- 46 ページの「Apex One サーバの場所」
- 47 ページの「サーバパフォーマンス」
- 48 ページの「インストール時に検索方法を指定」
- 49 ページの「ネットワークトラフィック」
- 51 ページの「他社製のセキュリティソフトウェア」
- 51 ページの「Active Directory」

新規インストールのすべての要件については、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Apex One サーバの場所

Apex One はさまざまなネットワーク環境に柔軟に対応できます。たとえば、Apex One サーバとエージェントの間にファイアウォールを設置したり、単一のネットワークファイアウォールの背後にサーバとすべてのエージェントを配置することができます。サーバとエージェントの間にファイアウォールを配置する場合は、エージェントとサーバの待機ポート間のトラフィックを許可するようにファイアウォールを設定してください。

ネットワークアドレス変換を使用するネットワークに配置したセキュリティエージェントの管理で発生する問題の解決方法については、管理者ガイドを参照してください。

重要

セキュリティ上の理由から、Apex One サーバは社内イントラネット内にインストールすることをお勧めします。ローカルイントラネット外のエンドポイントを管理する必要がある場合、トレンドマイクロでは、DMZ に Apex One エッジリレーサーバをインストールすることをお勧めします。

サーバパフォーマンス

大規模なネットワーク環境では、中小規模のネットワーク環境に比べ、サーバに対してより高い性能が要求されます。

ヒント

トレンドマイクロでは、Apex One サーバに、最低でも 2 GHz のデュアルプロセッサと、3 GB 以上の RAM を推奨しています。

1 つの Apex One サーバで管理できるネットワーク上のエンドポイントエージェントの数は、使用可能なサーバリソースやお使いのネットワークトポロジなど、複数の要因によって異なります。お使いのサーバで管理できるエージェント数については、トレンドマイクロの販売代理店にお問い合わせください。

専用サーバ

Apex One サーバをインストールするエンドポイントを選択するときは、次の点を考慮してください。

- エンドポイントの CPU 処理量
- エンドポイントで他の機能が実行されるかどうか

対象エンドポイントで他の機能が実行される場合は、重要なアプリケーションやリソースを大量に消費するアプリケーションを実行していない別のエンドポイントを選択してください。

インストール時に検索方法を指定

このバージョンの Apex One では、スマートスキャンまたは従来型スキャンのいずれかを使用するようにエージェントを設定できます。

従来型スキャン

従来型スキャンは、以前のすべての Apex One バージョンで使用されていた検索方法です。従来型スキャンエージェントでは、エージェントエンドポイント上にすべての Apex One コンポーネントが格納され、ローカルのすべてのファイルが検索されます。

スマートスキャン

スマートスキャンは、クラウドに格納された脅威のシグネチャを活用します。スマートスキャンモードでは、まず Apex One エージェントがローカルでセキュリティリスクを検索します。エージェントでファイルの危険性を判定できない場合には、Smart Protection Server に接続します。

スマートスキャンには、次の機能や利点があります。

- クラウド内での高速でリアルタイムなセキュリティステータスルックアップ機能 (自身のセキュリティステータスを確認する機能) の提供
- 新たな脅威に対する保護を提供するのにかかる全体時間の短縮
- パターンファイルのアップデートで消費されるネットワーク帯域幅の削減。パターン定義のアップデートのほとんどはクラウドにのみ配信すればよく、大量のエージェントに配信する必要はありません。
- 企業全体のパターン配信に伴うコストとオーバーヘッドの削減
- エンドポイントにおけるカーネルメモリ消費量の低下。消費量は最小限の範囲でゆっくり増加していきます。

検索方法の設定

新規インストールの場合、エージェントの初期設定の検索方法はスマートスキャン方式です。Apex One では、サーバのインストール後にドメインごとに

検索方法をカスタマイズすることもできます。次の点について考慮してください。

- サーバのインストール後に検索方法を変更していない場合は、インストールするすべてのエージェントでスマートスキャンが使用されます。
- すべてのエージェントで従来型スキャンを使用するには、サーバのインストール後にルートレベルの検索方法を従来型スキャンに変更してください。
- 従来型スキャンとスマートスキャンの両方を使用する場合は、ルートレベルの検索方法をスマートスキャンのままにして、従来型スキャンを適用するドメインに対して検索方法を変更することをお勧めします。

ネットワークトラフィック

配信について計画する際は、Apex One で生成されるネットワークトラフィックを考慮してください。次の場合、サーバによってトラフィックが生成されます。

- トレンドマイクロのアップデートサーバに接続し、最新のコンポーネントの有無を確認してダウンロードするとき
- 最新のコンポーネントをダウンロードするようにエージェントに通知するとき
- エージェントに設定の変更を通知するとき

次の場合、セキュリティエージェントでトラフィックが生成されます。

- 起動時
- コンポーネントをアップデートするとき
- 設定のアップデート時、および HotFix のインストール時
- セキュリティリスクの検索時
- 「スタンドアロン」モードと「標準」モードを切り替えるとき
- 従来型スキャンとスマートスキャンを切り替えるとき

コンポーネントアップデート時のネットワークトラフィック

Apex One は、コンポーネントのアップデート時に大量のネットワークトラフィックを生成します。コンポーネントのアップデート時に生じるネットワークトラフィックを軽減するために、Apex One ではコンポーネントを複製します。アップデートされたフルパターンファイルをダウンロードする代わりに、サイズの小さい「差分」パターンファイルのみをダウンロードし、現行のパターンファイルに統合します。

定期的にアップデートされているセキュリティエージェントは、差分パターンファイルのみをダウンロードします。定期的にアップデートされていない場合は、フルパターンファイルがダウンロードされます。

トレンドマイクロでは定期的に新しいパターンファイルを公開しています。さらに、被害を及ぼし、かつ活発に拡散されているウイルス/不正プログラムが発見された場合、ただちに新しいパターンファイルを公開します。

アップデートエージェントとネットワークトラフィック

エージェントと Apex One サーバ間のネットワークに、帯域幅の低い箇所またはトラフィックが多い箇所が存在する場合、一部の Apex One エージェントをアップデートエージェント (その他のエージェントのアップデート元) として指定することができます。これによって、すべてのエージェントへのコンポーネント配信の負担を分散できます。

たとえば、20 台以上のエンドポイントが配置されたリモートオフィスがある場合は、アップデートエージェントを指定して、Apex One サーバからのアップデートを複製し、ローカルネットワークの他のエージェントエンドポイントの配布ポイントとして使用します。アップデートエージェントの詳細については、管理者ガイドを参照してください。

Apex Central とネットワークトラフィック

Trend Micro Apex Central™は、ゲートウェイ、メールサーバ、ファイルサーバ、およびデスクトップ向けのトレンドマイクロ製品およびサービスを管理します。Apex Central は Web ベースの管理コンソールであり、ネットワークを介して製品およびサービスを一元的に監視できます。

Apex Central を使用して、1 ヵ所から複数の Apex One サーバを管理します。高速かつ安全なインターネット接続が設定された Apex Central サーバは、ト

レンドマイクロのアップデートサーバからコンポーネントをダウンロードできます。次に、Apex Central は安全ではないインターネットに接続された、またはインターネットに接続できない、Apex One サーバにコンポーネントを配信します。

詳細については、Apex Central のドキュメントを参照してください。

他社製のセキュリティソフトウェア

Apex One サーバをインストールするエンドポイントから、他社製のエンドポイントセキュリティソフトウェアを削除してください。Apex One サーバのインストールを妨げたり、パフォーマンスに影響する可能性があります。他社製のセキュリティソフトウェアを削除したら、エンドポイントをセキュリティリスクから保護するために、すぐに Apex One サーバおよびセキュリティエージェントをインストールしてください。

注意

Apex One では、他社製ウイルス対策製品のサーバコンポーネントを自動的にアンインストールすることはできませんが、エージェントコンポーネントはアンインストールできます。詳細については、管理者ガイドを参照してください。

Active Directory

役割ベースの管理およびセキュリティコンプライアンスの機能を利用するためには、すべての Apex One サーバが Active Directory ドメインに属している必要があります。

サイレントインストール

注意

この機能は現在日本では提供されていません。

複数の Apex One サーバで同一のインストール設定を使用する場合は、サーバをサイレントモードでインストールまたはバージョンアップします。

サイレントインストールの準備

手順

1. セットアップを起動してインストール設定を.iss ファイルに記録し、応答ファイルを作成します。応答ファイルを使用したサイレントインストールを実行するすべてのサーバで、記録した設定内容が使用されます。

   重要

   - セットアップは、ローカルインストールでのみ画面を表示します。
   - 新規インストールの場合は、Apex One サーバがインストールされていないエンドポイントから応答ファイルを作成してください。

2. コマンドプロンプトからセットアップを実行し、サイレントインストールに使用する応答ファイルの場所を指定します。

応答ファイルへのセットアップ設定の記録

この手順では、Apex One がインストールされるわけではありません。セットアップ設定を応答ファイルに記録するだけです。

手順

1. ApexOne.exe ファイルをダウンロードし、内容を展開します。
2. コマンドプロンプトを開き、Apex One の setup.exe ファイルがあるディレクトリを入力します。

   たとえば、「`CD C:\Apex One Installer\setup.exe`」と入力します。

3. 次のように入力します。

   ```
   setup.exe -r
   ```

-r パラメータを指定することで、セットアップが起動し、インストールの詳細が応答ファイルに記録されます。

4. セットアップウィザードでは、インストール操作を進めてください。
5. ウィザードの手順が完了したら、%windir%に作成された応答ファイル setup.iss を確認します。

サイレントインストールの実行

手順

1. 対象エンドポイントにインストールパッケージと setup.iss をコピーします。
2. 対象エンドポイントでコマンドプロンプトを開き、インストールパッケージのディレクトリを入力します。
3. 次のように入力します。

   ```
   setup.exe -s <-f1 パス>setup.iss <-f2 パス>setup.log
   ```

   例:C:¥setup.exe -s -f1C:¥setup.iss -f2C:¥setup.log

   説明:

   - -s:セットアップを起動してサイレントインストールを実行します。
   - <-f1 パス>setup.iss: 応答ファイルの場所。パスにスペースが含まれている場合は、パスを引用符 (") で囲ってください。たとえば次のように指定します。-f1"C:¥osce script¥setup.iss"
   - <-f2 パス>setup.log: インストール後に作成されるログファイルの場所。パスにスペースが含まれている場合は、パスを引用符 (") で囲ってください。たとえば次のように指定します。-f2"C:¥osce log¥setup.log"

4. <Enter> キーを押します。

   エンドポイントにサーバがサイレントインストールされます。

5. インストールが正常に行われたかどうかを確認するには、次の手順を実行します。
   - 対象エンドポイントで Apex One プログラムショートカットを確認します。ショートカットが作成されていない場合は、再度インストールを試みてください。
   - Apex One Web コンソールにログオンします。

セットアッププログラム

Apex One サーバのインストールを開始する準備ができたら、セットアッププログラムを実行します。

Apex One サーバの新規インストールを開始する前に、インストール先の環境が適切に準備されていることを確認してください。新規インストールの考慮事項の詳細については、以下を参照してください。

- 46 ページの「新規インストールの注意事項」
- 24 ページの「Apex Central の拡張機能の要件」

開始する準備が整っていることを確認したら、画面の指示に従って Apex One サーバをインストールします。

使用許諾契約書

インストールを続行するには使用許諾契約をお読みいただき、使用許諾契約の条項に同意いただく必要があります。使用許諾契約の条項に同意いただけない場合には、インストールを続行することはできません。

エンドポイントの事前検索

Apex One サーバのインストールを開始する前に、セットアップで対象エンドポイントのウイルスおよび不正プログラムを検索できます。セットアップで検索されるのは、エンドポイントの最も脆弱な次の場所です。

- システム領域とシステムディレクトリ (システム領域感染型ウイルスが対象)
- Windows フォルダ
- Program Files フォルダ

検出されたウイルス/不正プログラムやトロイの木馬プログラムに対しては、次の処理が実行されます。

- 削除: 感染したファイルを削除します。
- 駆除: 駆除できるファイルはフルアクセスを許可する前に駆除し、駆除できないファイルは次のいずれかの選択された処理を実行します。
- 拡張子変更: 感染ファイルの拡張子を「vir」に変更します。ユーザはそのままではファイルを開くことはできませんが、特定のアプリケーションと関連づければ開くことは可能です。ただし拡張子を変更した感染ファイルを開くと、ウイルス/不正プログラムが作動する可能性があります。
- 放置 (ログのみ): 感染ファイルに対して何もしないでフルアクセスを許可します。ユーザはそのファイルをコピー、削除、または開くことができます。

重要

ローカルのバージョンアップインストールの場合は、ランサムウェアの脅威に対する最新の保護が適用されるよう、ランサムウェア対策設定をアップデートするように求められます。

アップデートされた設定を適用した場合、挙動監視がすでに有効になっているエージェントの設定のみが変更されます。

プロキシサーバ

Apex One サーバはエージェント/サーバ間通信に HTTPS プロトコルを使用し、トレンドマイクロのアップデートサーバに接続してアップデートをダウンロードします。プロキシサーバでネットワークのインターネットトラフィックを処理しいる場合、Apex One サーバがアップデートをトレンドマイ

クロのアップデートサーバからダウンロードできるプロキシ設定が必要です。

インストール時にプロキシの設定をスキップして、インストール後に Apex One Web コンソールから指定することもできます。

製品のアクティベーション

受信済みのアクティベーションコード (大文字と小文字が区別されます) を指定して、Apex One の機能をすべてアクティベートします。

アクティベーションコードを取得するには、[オンライン登録] をクリックします。トレンドマイクロの製品登録 Web サイトが表示されます。登録フォームへの入力を完了すると、トレンドマイクロからメールでアクティベーションコードが送られてきます。受け取ったコードを使用して、インストールプロセスを続行してください。

製品バージョン

Apex One の製品版または体験版のいずれかをインストールできます。製品版、体験版にはそれぞれ異なる種類のアクティベーションコードが必要です。アクティベーションコードを入手するには、ユーザ登録が必要です。

表 2-1. バージョンの比較

バージョン	説明
製品版	製品版では、すべての製品機能とテクニカルサポートが提供されます。サポート契約失効後の更新猶予期間 (通常 90 日) も設定されています。更新猶予期間を過ぎると、テクニカルサポートやアップデートされたコンポーネントの提供を受けられなくなります。その場合、検索エンジンでは、古いバージョンのパターンファイルを使用して検索が行われます。これらの旧版コンポーネントでは、最新のセキュリティリスクから完全には保護できない可能性があります。その場合、サポート契約を更新してください。

バージョン	説明
体験版	体験版は、いつでも製品版にアップグレードできます。体験期間終了までに製品版にバージョンアップしないと、コンポーネントのアップデートや検索など、Apex One のすべてのエージェント機能が使用できなくなります。

レジストレーションキーおよびアクティベーションコード

インストール時に、アクティベーションコードを指定してすべての機能をアクティベートします。

アクティベーションコードをお持ちでない場合は、製品付属のレジストレーションキーを使用して取得してください。トレンドマイクロの製品登録 Web サイトに自動的にリダイレクトされます。

ユーザ登録後、トレンドマイクロからアクティベーションコードが送信されます。

インストール時に利用できるレジストレーションキーもアクティベーションコードもお持ちでない場合は、トレンドマイクロの販売代理店にお問い合わせください。

詳細については、125 ページの「製品サポート情報」を参照してください。

注意

登録については、次の Web サイトを参照してください。

https://esupport.trendmicro.com/support/viewxml.do?ContentID=en-116326

インストールパス

初期設定のインストールパスを使用するか、新しいパスを指定します。

サーバの識別

セキュリティエージェントによるサーバコンピュータの識別方法を、完全修飾ドメイン名 (FQDN)、ホスト (ドメイン) 名、IP アドレスの中から選択します。

IP アドレスを指定した場合、サーバコンピュータとセキュリティエージェントの間の通信はその IP アドレスに依存します。IP アドレスを変更すると、セキュリティエージェントは Apex One サーバと通信できなくなります。この場合、通信を復元するには、すべてのセキュリティエージェントを配信し直すしかありません。サーバコンピュータをホスト名で識別している場合にホスト名を変更した場合も同様です。

ほとんどのネットワークでは、サーバコンピュータの IP アドレスはホスト名に比べて変更される可能性が高いため、一般にはホスト名で識別することをお勧めします。

ヒント

ホスト名の代わりに IP アドレスを使用している場合、インストール後に IP アドレス (DHCP サーバから取得) を変更することは避けてください。DHCP サーバから取得した IP アドレス情報をそのまま使用するように IP アドレス設定を設定することで、セキュリティエージェントとの以降の通信の問題を回避できます。

IP アドレス設定を保持するもう 1 つの方法は、その IP アドレスを Apex One サーバ専用にすることです。これにより、DHCP が有効な場合でも、DHCP サーバから Apex One に同じ IP アドレスが割り当てられます。

静的 IP アドレスを使用している場合は、サーバを IP アドレスで識別します。さらに、サーバコンピュータに複数のネットワークインタフェースカード (NIC) が搭載されている場合には、エージェント/サーバ間の通信が成功するよう、ホスト名ではなく IP アドレスの 1 つを使用することを検討してください。

Web サーバ

Apex One Web サーバは Web コンソールをホストし、管理者にコンソールの Common Gateway Interface (CGI) の実行を許可し、セキュリティエージェン

トからの命令を受け入れます。Web サーバは、この命令をセキュリティエージェントの CGI に変換し、Apex One Master Service に転送します。

HTTP ポート

Web サーバは、セキュリティエージェントの要求を HTTP ポートで待機し、Apex One Master Service に要求を転送します。Apex One Master Service は、セキュリティエージェントの指定された通信ポート経由でセキュリティエージェントに情報を返します。

SSL サポート

Apex One では、Web コンソールとサーバ間の通信をセキュリティで保護するために SSL (Secure Socket Layer) を使用します。SSL は、ハッカーに対するさらなる保護を提供します。Apex One では、Web コンソールで指定されたパスワードが Apex One サーバへ送信される前に暗号化されますが、ハッカーはパケットを盗聴することで、復号することなく「再現」してコンソールにアクセスすることができます。SSL トンネリングによって、ネットワークで送信されるパケットをハッカーが盗聴するのを防ぐことができます。

使用する SSL バージョンは、Web サーバがサポートするバージョンに応じて異なります。

SSL を選択した場合、SSL 接続に必須の SSL 証明書がセットアップによって自動的に作成されます。証明書には、サーバ情報、公開鍵、および秘密鍵が含まれています。

SSL 証明書には 1～20 年の有効期間が指定されている必要があります。管理者は期限切れの証明書を使用することはできます。ただし、同じ証明書を使用して SSL 接続を要求するたびに警告メッセージが表示されます。

SSL を使用した通信の動作

1. 管理者は情報を Web コンソールから SSL 接続経由で Web サーバに送信できます。
2. Web サーバは、必要な証明書を使用する Web コンソールに応答します。
3. ブラウザは、RSA 暗号化を使用して鍵の交換を実行します。

4. Web コンソールは、Web サーバに RC4 暗号化を使用してデータを送信します。

RSA 暗号化は安全性は高いですが通信速度が低下します。したがって、この方式は鍵交換のみに使用し、より高速な代替方式である RC4 をデータ転送に使用します。

Web サーバのポート

次の表は、Web サーバの初期設定のポート番号を示しています。

表 2-2. Apex One Web サーバのポート番号

Web サーバと設定	ポート番号	
	HTTP	HTTPS (SSL)
IIS 既定 Web サイトで SSL が有効	80 (設定不可)	443 (設定不可)
IIS 仮想 Web サイトで SSL が有効	8080 (設定可能)	4343 (設定可能)

Endpoint Sensor のインストール

Apex Central と統合する場合で、Endpoint Sensor ライセンスの購入が済んでいるときは、[Endpoint Sensor のインストール] を選択してセキュリティエージェントで必要な Endpoint Sensor サービスがすべて利用できることを確認します。

注意

この機能が公式にサポートされているのは次のプラットフォームのみです。

- Windows 7 SP1
- Windows 8.1
- Windows10

次の表では、Endpoint Sensor サービスのインストールに必要な最小要件を示しています。

項目	要件	確認
Redis サービス	Apex One サーバコンピュータには、既存の Redis サービスをインストールできません。既存の Redis サービスをアンインストールしてから、セットアッププログラムを使用して新しいサービスをインストールする必要があります。	[Endpoint Sensor のインストール] 画面で [次へ] をクリックした後
SQL Server のバージョン	• SQL Server 2017 • SQL Server 2016 SP1 **注意** この機能では、SQL Server Express のバージョンはサポートされていません。	[Apex One データベースセットアップ] 画面で [次へ] をクリックした後
データベース設定	[検索のためのフルテキスト抽出とセマンティック抽出] を有効にする [検索のためのフルテキスト抽出とセマンティック抽出] の有効化の詳細については、SQL Server のドキュメントを参照してください。	[Apex One データベースセットアップ] 画面で [次へ] をクリックした後
	データベースメンテナンス機能を使用するための tempdb データベースへのアクセス権	なし

注意

Endpoint Sensor サービスをインストールしなかった場合や、[検索のためのフルテキスト抽出とセマンティック抽出] が有効になっているサポート対象のバージョンの SQL Server を選択しなかった場合に、Endpoint Sensor を後で使用するには、Windows の [コントロール パネル] にある [プログラムのアンインストールまたは変更] にアクセスする必要があります。

Apex One サーバを選択して、[変更] をクリックします。

Apex One データベースセットアップ

重要

Endpoint Sensor 機能の使用を検討している場合は、適切に準備された、サポートされているバージョンの SQL Server でデータベースを作成する必要があります。

詳細については、29 ページの「Apex One Endpoint Sensor」を参照してください。

手順

1. Apex One データベースの場所を選択します。
   - 新しい SQL Server Express インスタンスのインストール/作成: SQL Server 2016 SP2 Express のインストールを選択し、「\OFFICESCAN」データベースインスタンスを作成します。

     重要

     このオプションは、Endpoint Sensor 機能をインストールする選択をした場合は利用できません。
   - SQL Server: Apex One で使用する既存の SQL Server とデータベースインスタンスを選択します。
2. データベースの認証方法を選択します。

   Windows アカウントを使用してサーバにログオンするときは、Apex One に現在ログオンしているユーザのユーザ名が適用されます。

重要

ユーザアカウントは、ローカル管理者グループに属しているか、Active Directory (AD) ビルトイン管理者である必要があります。また、Windows のローカルセキュリティポリシーまたはグループポリシー管理コンソールを使用して、次のユーザ権限割り当てポリシーを設定する必要があります。

- サービスとしてログオン
- バッチジョブとしてログオン
- ローカルログオンを許可

ユーザアカウントには、次に示すデータベースの役割も必要です。

- dbcreator

  注意

  セットアッププログラムを使用して新しいデータベースインスタンスを作成した場合のみ必要です。

- bulkadmin
- db_owner

3. [データベース名] セクションで、所定の Apex One データベースで使用する、SQL Server 上のデータベースインスタンスの名前を指定します。

注意

- [Endpoint Sensor] オプションは、Endpoint Sensor 機能のインストールを選択した場合にのみ表示されます。
- SQL Server 上に指定したデータベースが存在しない場合は、新しいデータベースインスタンスが、セットアッププログラムにより自動的に作成されます。設定済みの認証アカウントで新しいデータベースを作成するには、dbcreator 権限が必要です。

Apex One セキュリティエージェント配信

セキュリティエージェントのインストールやバージョンアップは、複数の方法で行うことができます。この画面には、各種の配信方法と、必要なネットワーク帯域幅の概算値が表示されます。

この画面を使用して、セキュリティエージェントを対象エンドポイントに配信するときにサーバに必要な容量や、消費される帯域幅を確認します。

注意

すべてのインストール方法で、対象エンドポイントのローカル管理者権限またはドメイン管理者権限が必要になります。

統合 Smart Protection Server のインストール

統合 Smart Protection Server は、セットアップを使用して対象エンドポイントにインストールすることができます。統合サーバは、スマートスキャンを使用するセキュリティエージェントにファイルレピュテーションサービスを提供し、Web レピュテーションポリシーが適用されるセキュリティエージェントに Web レピュテーションサービスを提供します。統合サーバは Apex One Web コンソールで管理します。

重要

このバージョンの Apex One では、ファイルレピュテーションおよび Web レピュテーションのクエリには HTTPS 通信のみをサポートしています。

スタンドアロンの Smart Protection Server をインストールすることをお勧めします。スタンドアロンの Smart Protection Server は、使用できる機能は統合サーバと同じですが、より多くのセキュリティエージェントに対応できます。スタンドアロンサーバは別途インストールされ、独自の管理コンソールを持ちます。スタンドアロンサーバについては、Trend Micro Smart Protection Server の管理者ガイドを参照してください。

ヒント

統合 Smart Protection Server と Apex One サーバは同じエンドポイント上で実行されるため、2 つのサーバのトラフィックがピークになるときには、エンドポイントのパフォーマンスが著しく低下する場合があります。Apex One サーバへのトラフィックを減らすには、スタンドアロン Smart Protection Server をプライマリ Trend Micro Smart Protection ソースとして割り当てて、統合サーバをバックアップソースとして割り当てます。セキュリティエージェントの Smart Protection ソースの設定については、管理者ガイドを参照してください。

統合サーバをインストールしない場合

新規インストールの実行時に統合サーバをインストールしないと、次のようになります。

- 従来型スキャンが初期設定の検索方法になります。
- 別のインストール画面 (69 ページの「Web レピュテーションサービス」を参照) で Web レピュテーションポリシーを有効にしても、Smart Protection Server がインストールされていないと判断されるため、エージェントから Web レピュテーションクエリを送信することはできません。

Apex One のインストール後にスタンドアロンサーバが使用可能な場合は、Apex One Web コンソールから次のタスクを実行します。

- 検索方法をスマートスキャンに変更します。
- スタンドアロンサーバを Smart Protection ソースリストに追加して、エージェントからサーバにファイルと Web レピュテーションクエリを送信できるようにします。

セキュリティエージェントのインストール

対象サーバにセキュリティエージェントをインストールする場合に選択します。

セキュリティリスクに対する保護を実際に提供するのは、セキュリティエージェントプログラムです。したがって、Apex One サーバコンピュータをセキュリティリスクから保護するためには、セキュリティエージェントプログ

ラムもサーバに必要です。サーバのインストール時にセキュリティエージェントをインストールするオプションを選択すると、サーバは自動的に保護されます。また、サーバのインストール後にセキュリティエージェントをインストールする手間も省けます。

注意

ネットワーク上の別のエンドポイントには、サーバのインストール後にセキュリティエージェントをインストールしてください。

詳細情報については、管理者ガイドを参照してください。

トレンドマイクロまたは他社製のエンドポイントセキュリティソフトウェアがサーバコンピュータにすでにインストールされている場合、そのソフトウェアを Apex One で自動的にアンインストールしてセキュリティエージェントと置き換えることができない場合があります。Apex One で自動的にアンインストールされるソフトウェアのリストについては、サポート担当者にお問い合わせください。ソフトウェアが自動的にアンインストールされない場合には、手動でアンインストールしてから Apex One のインストールを続行してください。

スマートフィードバック

トレンドマイクロスマートフィードバックは、トレンドマイクロのテクノロジおよび 24 時間体制の TrendLabs の運用によって、トレンドマイクロの製品間での継続的な情報交換を実現しています。ユーザの 1 回の定期的なレピュテーションチェックによって新しい脅威が特定されるたびに、トレンドマイクロの脅威に関するデータベースがすべて自動的にアップデートされ、これ以降ユーザで所定の脅威が発生することがないようブロックされます。

顧客およびパートナーの広範囲にわたる世界的なネットワークを通して収集された脅威に関する情報を継続的に処理することによって、トレンドマイクロは、最新の脅威に対して自動的なリアルタイムの保護を提供し、住民を保護するために地域で行われる自動化された自警組織と同様に、「団結」することによるセキュリティの強化を実現しています。脅威に関して収集される情報は、特定の通信のコンテンツではなく、送信元の評価に基づいています。

トレンドマイクロに送信される情報のサンプルを次に示します。

- ファイルのチェックサム
- アクセスされた Web サイト
- サイズやパスなどのファイル情報
- 実行可能ファイルの名前

プログラムへの参加は、Web コンソールからいつでも終了できます。

ヒント

ご使用のエンドポイントを保護するためにスマートフィードバックに参加することは必須ではありません。参加は任意であり、いつでも参加の取り消しができます。トレンドマイクロ製品のすべてのお客さまに対する全体的な保護の強化に役立つので、スマートフィードバックへの参加をお勧めします。

Trend Micro Smart Protection Network の詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

セキュリティエージェントのインストール

初期設定のセキュリティエージェントインストール設定をそのまま使用するか、別のインストールパスを指定します。インストールディレクトリに十分なディスクの空き容量がない場合には、パスを変更します。

ヒント

初期設定を使用することを推奨します。

別のインストールパスを指定する場合、静的パスを入力するか変数を使用します。ディレクトリが指定したパスのディレクトリがセキュリティエージェント上に存在しない場合には、セキュリティエージェントインストール時に自動的にディレクトリが作成されます。

セキュリティエージェントインストールパスを固定パスで入力するには、ドライブ文字を含めたドライブパスを入力します。たとえば、C:¥Program Files¥Trend Micro¥Security Agent のようになります。

注意

セキュリティエージェントのインストールパスは、Apex One サーバのインストール完了後に変更することはできません。インストールされるすべてのセキュリティエージェントで同じインストールパスが使用されます。

セキュリティエージェントインストールパスに変数を指定する場合には、次の変数を使用します。

- $BOOTDISK: エンドポイントが起動するハードディスクのドライブ文字。初期設定は C:¥です。
- $WINDIR:Windows ディレクトリ。初期設定は C:¥Windows です。
- $ProgramFiles:Program Files ディレクトリは Windows で自動的に設定され、通常はソフトウェアのインストール先として使用されます。初期設定は C:¥Program Files です。

また、この画面では次の設定をします。

- ポート番号: Apex One サーバは指定したポートを使用してエージェントと通信します。初期設定値を受け入れるか、新しい値を入力します。

Apex One ファイアウォール

Apex One のファイアウォールは、ステートフルインスペクション、高性能なネットワークウイルス検索、および駆除機能を使用して、ネットワーク上のセキュリティエージェントとサーバを保護します。IP アドレス、ポート番号、プロトコルなどによって接続をフィルタする複数のルールを作成し、それらのルールを異なるユーザのグループに適用します。

Apex One ファイアウォールを無効にして、後で Apex One サーバの Web コンソールから有効にすることもできます。

必要に応じて、サーバプラットフォームの Apex One ファイアウォールを有効にします。バージョンアップ時にサーバプラットフォームで Apex One ファ

イアウォールがすでに有効になっている場合は、[Apex One ファイアウォールを有効にする (サーバプラットフォーム)] を選択して、バージョンアップ後に Apex One で Apex One ファイアウォールが無効にならないようにします。

スパイウェア対策機能

診断モードでは、サーバの管理対象のすべてのエージェントで、手動検索、予約検索、リアルタイム検索、および ScanNow で検出されたスパイウェア/グレーウェアがログに記録されますが、スパイウェア/グレーウェア自体は駆除されません。

トレンドマイクロの診断モードは、トレンドマイクロが検出したスパイウェア/グレーウェアを評価し、その結果に基づいて管理者が適切な処理を実行できるようにする機能です。たとえば、検出されたスパイウェア/グレーウェアがセキュリティリスクではないと見なされる場合には、スパイウェア/グレーウェアの承認済みリストに追加できます。

診断モードで推奨されているいくつかの処理については、インストール後に管理者ガイドを参照してください。

診断モードが特定の期間にのみ適用されるように設定するには、この画面で週単位の期間を指定します。診断モードの設定は、インストール後に Web コンソール ([エージェント] > [グローバルエージェント設定] の [スパイウェア/グレーウェア設定] セクションの [セキュリティ設定] タブ) で変更できます。

Web レピュテーションサービス

Web レピュテーションポリシーによって、Apex One が Web サイトへのアクセスをブロックするか許可するかが決まります。ポリシーの詳細については、管理者ガイドを参照してください。

[Web レピュテーションサービスを有効にする (デスクトッププラットフォーム)] を選択すると、デスクトッププラットフォームにインストールされている内部および外部のエージェントに対してポリシーが有効になります。サーバプラットフォームでデスクトッププラットフォームと同レベルの Web セキュリティを必要とする場合は、[Web レピュテーションサービスを有効にする (サーバプラットフォーム)] を選択します。

セキュリティエージェントは、Web コンソールの [エンドポイントの位置] 画面で設定された位置基準を使用して、エンドポイントの位置と適用されるポ

リシーを判断します。セキュリティエージェントのポリシーは、位置が変わるたびに切り替えられます。

Web レピュテーションポリシーは、インストール後に Web コンソールから設定します。通常は、外部エージェントに対してより厳格なポリシーを設定します。

Web レピュテーションポリシーは、Apex One エージェントツリーで細かく設定されます。ポリシーは、すべてのエージェント、エージェントグループ、または個別のエージェントに適用できます。

Web レピュテーションポリシーを有効にする場合は、必ず Smart Protection Server (統合またはスタンドアロン) をインストールして、Apex One Web コンソールの Smart Protection ソースリストに追加してください。セキュリティエージェントからこのサーバに Web レピュテーションクエリが送信され、ユーザがアクセスしている Web サイトの安全性が確認されます。

注意

統合サーバは、Apex One サーバと一緒にインストールされます。詳細については、64 ページの「統合 Smart Protection Server のインストール」を参照してください。スタンドアロンサーバは別途インストールします。

サーバ認証証明書

インストール中、セットアッププログラムは既存の認証証明書がないか検出を試みます。既存の証明書があった場合、そのファイルが [サーバ認証証明書] 画面に自動的に表示されます。既存の証明書がない場合は、初期設定で [新しい認証証明書を生成する] オプションが選択されます。

Apex One では、公開鍵暗号法を使用して、Apex One サーバからエージェントへの通信を認証します。公開鍵暗号法では、サーバは秘密鍵を保持し、すべてのエージェントに公開鍵を配布します。エージェントは、公開鍵を使用して、受信する通信がサーバから開始された有効なものかどうかを検証します。検証に成功した場合、エージェントは応答します。

注意

Apex One では、エージェントからサーバへの通信は、サーバ側では認証されません。

Apex One のインストール時に認証証明書を生成することも、別の Apex One サーバから既存の認証証明書をインポートすることもできます。

管理者アカウントのパスワード

Web コンソールへのアクセス、およびセキュリティエージェントのアンロード/アンインストールで使用するパスワードを指定します。

Web コンソールへのアクセス

インストール時にセットアップによってルートアカウントが作成されます。ルートアカウントには、Apex One Web コンソールのすべての機能へのフルアクセスがあります。管理者は、このアカウントを使用してログオンすることで、他のユーザが Web コンソールへログオンするために使用できるカスタムユーザアカウントを作成できます。ユーザが設定または表示できる Web コンソールの機能は、アカウントのアクセス権限によって決まります。

指定したパスワードは、Apex One 管理者以外のユーザには知られないようにしてください。パスワードを忘れた場合の再設定については、サポート担当者にお問い合わせください。

セキュリティエージェントのアンロードとアンインストール

セキュリティエージェントのアンインストールやアンロードが無許可で行われないように、パスワードを指定します。セキュリティエージェントのアンインストールやアンロードは、セキュリティエージェントの機能に問題がある場合にのみ実行し、すぐにインストール/再ロードを行ってください。

Apex One プログラムショートカット

プログラムショートカットを表示するフォルダとして、初期設定のフォルダをそのまま使用するか、新しいフォルダを指定するか、または既存のフォルダを選択します。

インストール情報

この画面は、インストール設定の概要を表示します。インストール情報が正しいことを確認し、[戻る] をクリックして設定やオプションを変更します。インストールを開始するには、[インストール] をクリックします。

InstallShield Wizard の完了

インストールが完了したら、製品の基本情報や既知の問題などが記載された Readme ファイルを確認してください。

以下の場所に、バックアップしたフォレンジックスフォルダとデータベースを復元します。

```
<Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥
```

管理者は、Web コンソールを起動して、Apex One の設定を開始できます。

第 3 章

Trend Micro Apex One のバージョンアップ

この章では、Trend Micro Apex One のバージョンアップ手順について説明します。

この章の内容

バージョンアップの注意事項

重要

Apex Central と Apex One サーバの同一 OS へのインストールは サポート されていません。

詳細については、https://success.trendmicro.com/jp/solution/000286643 を参照してください。

このバージョンの Apex One Service Pack 1 では、Apex One からのバージョンアップがサポートされています。

注意

トレンドマイクロでは、バージョンアップの実行前に、すべての利用可能なパッチおよび HotFix を現在の Apex One サーバに適用することを強くお勧めしています。

Apex One システム要件の完全なリストについては、次の Web サイトを参照してください。

http://www.go-tm.jp/corp/req

Apex One サーバおよびセキュリティエージェントをバージョンアップするときには、次の点に注意してください。

- 74 ページの「IPv6 のサポート」
- 75 ページの「Trend Micro Apex One の設定」
- 77 ページの「バージョンアップ時に検索方法を指定」

IPv6 のサポート

Apex One サーバおよびエージェントのバージョンアップにおける IPv6 の要件は次のとおりです。

- サーバは IIS Web サーバを使用している必要があります。

- IPv6 アドレスをサーバに割り当てます。また、サーバはホスト名で識別する必要があります。完全修飾ドメイン名 (FQDN) を使用することをお勧めします。サーバが IPv6 アドレスで識別されている場合は、そのサーバが現在管理しているすべてのエージェントとサーバとの接続が切断されます。サーバが IPv4 アドレスで識別されている場合は、IPv6 エンドポイントにエージェントを配信することはできません。
- `ping` や `nslookup` コマンドなどを使用して、ホストコンピュータの IPv6 または IPv4 アドレスを取得できることを確認してください。

Trend Micro Apex One の設定

Trend Micro Apex One サーバをバージョンアップする場合は、Trend Micro Apex One データベースと重要な設定ファイルをバックアップしておきます。

ヒント

このバージョンの Trend Micro Apex One には、ロールバック用にバックアップメカニズムが用意されています。インストール時に自動バックアップを使用しない場合は、データベースの手動バックアップを実行してください。

Apex One データベースと設定ファイルのバックアップと復元

手順

1. Microsoft 管理コンソールで、Apex One Master Service を停止します。
2. Apex One Apex Central Agent サービスを停止します。
3. Apex One プラグインマネージャサービスを停止します。
4. World Wide Web Publishing サービスを停止します。
5. `<サーバのインストールフォルダ>¥¥PCCSRV¥¥Admin¥¥Utility¥¥SQ` フォルダにある次のデータベースファイルを手動でバックアップします。
   - `libSQLDatabaseUpgrade.dll`
   - `oscedbt.exe`

6. <サーバのインストールフォルダ>¥PCCSRV フォルダにある次のファイルとフォルダを手動でバックアップします。

   注意

   バージョンアップで問題が発生した場合にのみ、これらのファイルとフォルダをバックアップして、Apex One をロールバックしてください。

   - ofcscan.ini:グローバルエージェント設定が含まれます。
   - ous.ini:ウイルス対策コンポーネント配信用のアップデート元情報が含まれます。
   - Private フォルダ: ファイアウォールとアップデート元設定が含まれます。
   - Web¥tmOPP フォルダ: 大規模感染予防設定が含まれます。
   - Pccnt¥Common¥OfcPfw*.dat:ファイアウォール設定が含まれます。
   - Download¥OfcPfw*.dat:ファイアウォール配信設定が含まれます。
   - Log フォルダ: システムイベントおよび接続状態の確認ログが含まれます。
   - Virus フォルダ: 隔離されたファイルが含まれます。
   - HTTPDB フォルダ: Apex One データベースが含まれます

7. Apex One サーバをバージョンアップします。

注意

バージョンアップで問題が発生した場合は、手順 6 のバックアップファイルを対象エンドポイントの<サーバのインストールフォルダ>¥¥PCCSRV フォルダにコピーして、次のサービスを再起動します。

- World Wide Web Publishing サービス
- Apex One プラグインマネージャサービス
- Apex One Apex Central Agent サービス
- Apex One Master Service

バージョンアップ時に検索方法を指定

このバージョンの Apex One では、管理者は、スマートスキャンまたは従来型スキャンのいずれかを使用するようにセキュリティエージェントを設定できます。

Apex One を以前のバージョンからバージョンアップする場合、選択したバージョンアップ方法に応じてドメインごとにバージョンアップ前の検索方法をそのまま使用するか、またはカスタマイズすることができます。次の点について考慮してください。

- サーバコンピュータ上で直接 Apex One サーバをバージョンアップする場合、エージェントではバージョンアップ後も検索方法の設定が保持されるため、検索方法を変更する必要はありません。
- Apex One Service Pack 1 サーバにセキュリティエージェントを移動することでバージョンアップを行う場合:
  - Apex One Service Pack 1 サーバで、エージェントグループを手動で設定します。この方法でエージェントグループを設定する場合、新しいドメインを作成できます。

    注意

    エージェントの自動グループ設定を使用する場合は、エージェントのバージョンアップ時にすべての検索設定が維持されるように、すべてのエージェントのバージョンアップが完了してから自動グループ設定を有効にしてください。

- 前バージョンの Apex One サーバのドメイン構造および検索方法設定を、Apex One Service Pack 1 サーバにコピーします。2 つのサーバのドメイン構造と検索方法設定が異なる場合、Apex One Service Pack 1 サーバに移動するセキュリティエージェントに、検索方法設定が適用されないことがあります。

サーバおよびエージェントのバージョンアップ前の注意事項

Apex One サーバとエージェントをバージョンアップする前に、以下の点に注意してください。

1. データの損失に備え、Apex One サーバで以下のフォレンジックスフォルダとデータベースのバックアップを手動で作成してください。

   - `<Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicData`
   - `<Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicDataTracker.db`

   重要

   以下のファイルの場所を記録します。バージョンアッププロセスが完了したら、フォレンジックスフォルダとデータベースを元の場所に復元します。

2. インストールパッケージには、ファイアウォールドライバのアップデートが含まれています。現在のサーバのバージョンで Apex One ファイアウォールを有効にしている場合、このパッケージを配信すると、以下のエージェントエンドポイントがネットワークから切断される可能性があります。

   - ファイアウォールドライバのアップデートが開始されると、エージェントエンドポイントが一時的にネットワークから切断されます。切断する際、ユーザへの通知は行われません。

     Apex One Web コンソールには、ファイアウォールドライバのアップデートをエージェントエンドポイントの再起動後まで延期するオプ

ションがあり、初期設定で有効になっています。切断の問題を回避するには、このオプションを有効にします。

このオプションの設定は、次の方法で確認できます。

a. [エージェント] > [グローバルエージェント設定] に移動し、[セキュリティ設定] タブをクリックします。

b. [ファイアウォール設定] セクションに移動します。オプションは [システムの再起動後に Apex One ファイアウォールドライバをアップデートする] です。

- パッケージの配信後も、エージェントエンドポイントには TDI ドライバの以前のバージョンがまだ存在します。新しいバージョンはエンドポイントを再起動するまでロードされません。すぐに再起動しない場合は、セキュリティエージェントの使用時に問題が発生する可能性があります。

  Web コンソールで再起動の通知メッセージを表示するオプションが有効になっていれば、再起動を求めるメッセージが表示されます。ただし、ユーザが後で再起動するように選択した場合、メッセージが再度表示されることはありません。このオプションが無効になっている場合、ユーザへの通知は行われません。

  再起動の通知メッセージを表示するオプションは、初期設定で有効になっています。このオプションの設定は、次の方法で確認できます。

  - a. [エージェント] > [グローバルエージェント設定] に移動し、[エージェント制御] タブをクリックします。

    b. [警告設定] セクションに移動します。[新しいカーネルモードドライバのロードに、エンドポイントの再起動が必要な場合は通知メッセージを表示] オプションが選択されていることを確認してください。

3. 以下の場合、このバージョンへの Apex One サーバのバージョンアップは行えません。

   - サーバのバージョンアップ時にエージェントでログオンスクリプト (`AutoPcc.exe`) が実行されている。サーバをバージョンアップする前に、ログオンスクリプトを実行しているエージェントがないことを確認してください。

- サーバでデータベース関連タスクが実行されている。バージョンアップを実行する前に、サーバデータベース (DbServer.exe) の状態を確認してください。たとえば、Windows タスクマネージャーを開き、DbServer.exe の CPU 使用率が「00」であることを確認します。CPU 使用率がこれよりも高い場合は、データベース関連タスクが完了して使用率が「00」になるまで待ちます。バージョンアップの実行時にエラーが発生する場合は、データベースファイルがロックされている可能性があります。この場合は、サーバコンピュータを再起動してファイルのロックを解除してから、再度バージョンアップを実行します。

次のいずれかのバージョンアップ方法を使用します。

- 80 ページの「バージョンアップ方法 1: エージェントの自動バージョンアップの無効化」
- 82 ページの「バージョンアップ方法 2: アップデートエージェントのバージョンアップ」
- 89 ページの「バージョンアップ方法 3: Apex One Service Pack 1 サーバへのエージェントの移動」
- 92 ページの「バージョンアップ方法 4: エージェントの自動バージョンアップの有効化」

バージョンアップ方法 1: エージェントの自動バージョンアップの無効化

エージェントの自動バージョンアップを無効にすると、サーバをバージョンアップした後、エージェントをグループ単位でバージョンアップできます。多数のエージェントをバージョンアップする場合はこのバージョンアップ方法を使用します。

パート 1: Apex One サーバでのアップデート設定

手順

1. [エージェント] > [エージェント管理] に移動します。

2. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックし、[その他の設定] タブに移動します。
4. [セキュリティエージェントがアップデートするコンポーネント] リストで、[パターンファイル] を選択します。
5. [すべてのエージェントに適用] をクリックします。

   ネットワーク環境が複雑な場合や、エージェント数が多い場合は、設定をオンラインエージェントに配信するのに時間がかかる場合があります。バージョンアップ前に、設定をすべてのエージェントに配信するのに十分な時間を割り当ててください。設定を適用していないセキュリティエージェントは自動的にバージョンアップされます。

パート 2: Apex One サーバのバージョンアップ

Apex One サーバのバージョンアップの詳細については、94 ページの「ローカルバージョンアップの実行」を参照してください。

インストールの完了後、エージェントをバージョンアップする前に、Web コンソールを使用して Apex One サーバを設定します。

Apex One の詳細な設定手順については、管理者ガイドまたはサーバのオンラインヘルプを参照してください。

パート 3: セキュリティエージェントのバージョンアップ

手順

1. [アップデート] > [エージェント] > [自動アップデート] に移動し、次のオプションが有効であることを確認します。
   - Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する

- 再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)

2. [エージェント] > [エージェント管理] に移動します。
3. エージェントツリーで、バージョンアップするエージェントを選択します。1 つまたは複数のドメインを選択するか、ドメイン内のすべてまたは個別のエージェントを選択できます。
4. [設定] > [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
5. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。
6. [保存] をクリックします。
7. バージョンアップの結果をチェックします。
   - 87 ページの「オンラインエージェント」
   - 88 ページの「オフラインエージェント」
   - 89 ページの「スタンドアロンエージェント」
8. エージェントエンドポイントを再起動して、エージェントのバージョンアップを終了します。
9. 手順 2～8 を繰り返して、すべてのエージェントをバージョンアップします。

バージョンアップ方法 2: アップデートエージェントのバージョンアップ

多数のエージェントをアップデートエージェントからバージョンアップする場合は、このバージョンアップ方法を使用します。各エージェントは、それぞれ個別のアップデートエージェントからバージョンアップされます。

アップデートエージェントからバージョンアップされないセキュリティエージェントは、Apex One サーバからバージョンアップされます。

パート 1: Apex One サーバでのアップデート設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを選択します。
3. [設定] > [権限とその他の設定] の順にクリックし、[その他の設定] タブに移動します。
4. [セキュリティエージェントがアップデートするコンポーネント] リストで、[パターンファイル] を選択します。
5. [すべてのエージェントに適用] をクリックします。

   ネットワーク環境が複雑な場合や、エージェント数が多い場合は、設定をオンラインエージェントに配信するのに時間がかかる場合があります。バージョンアップ前に、設定をすべてのエージェントに配信するのに十分な時間を割り当ててください。設定を適用していないセキュリティエージェントは自動的にバージョンアップされます。

パート 2: Apex One サーバのバージョンアップ

Apex One サーバのバージョンアップの詳細については、94 ページの「ローカルバージョンアップの実行」を参照してください。

インストールの完了後、エージェントをバージョンアップする前に、Web コンソールを使用して Apex One サーバを設定します。

Apex One の詳細な設定手順については、管理者ガイドまたはサーバのオンラインヘルプを参照してください。

パート 3: アップデートエージェントのバージョンアップ

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、バージョンアップするアップデートエージェントを選択します。

   ヒント

   アップデートエージェントを簡単に見つけるには、ドメインを選択して、エージェントツリー上部の [エージェントツリー表示] から [アップデートエージェント表示] を選択します。

3. [設定] > [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
4. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。
5. [保存] をクリックします。
6. [アップデート] > [エージェント] > [手動アップデート] に移動します。
7. [エージェントを手動で選択] オプションを選択し、[選択] をクリックします。
8. 表示されたエージェントツリーで、バージョンアップするアップデートエージェントを選択します。

   ヒント

   アップデートエージェントを簡単に見つけるには、ドメインを選択して、エージェントツリー上部の [エージェントツリー表示] から [アップデートエージェント表示] を選択します。

9. エージェントツリーの上部にある [アップデートを開始] をクリックします。

10. バージョンアップ結果を確認します。
    - オンラインのアップデートエージェントは、コンポーネントのアップデートが開始されるとただちにバージョンアップされます。
    - オフラインのアップデートエージェントは、オンラインになったときにバージョンアップされます。
    - スタンドアロンのアップデートエージェントは、オンラインになったときにバージョンアップされるか、アップデートエージェントにバージョンアップ権限がある場合には、予約アップデートの実行時にバージョンアップされます。
11. アップデートエージェントのエンドポイントを再起動して、エージェントのバージョンアップを終了します。
12. 手順 1～11 を繰り返して、すべてのアップデートエージェントをバージョンアップします。

パート 4: アップデートエージェントの設定

手順

1. [エージェント] > [エージェント管理] に移動します。
2. エージェントツリーで、バージョンアップするアップデートエージェントを選択します。

   ヒント

   アップデートエージェントを簡単に見つけるには、ドメインを選択して、エージェントツリー上部の [エージェントツリー表示] から [アップデートエージェント表示] を選択します。
3. アップデートエージェントに最新のコンポーネントがインストールされていることを確認します。
4. [設定] > [アップデートエージェント設定] の順にクリックします。
5. 次のオプションを選択します。

- コンポーネントのアップデート
- ドメイン設定
- セキュリティエージェントプログラムと HotFix

6. [保存] をクリックします。

   アップデートエージェントによるエージェントプログラムのダウンロードが完了したら、パート 5 に進みます。

7. 手順 1～6 を繰り返して、すべてのアップデートエージェントに必要な設定を適用します。

パート 5: セキュリティエージェントのバージョンアップ

手順

1. [アップデート] > [エージェント] > [自動アップデート] に移動し、次のオプションが有効であることを確認します。
   - Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する
   - 再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)
2. [エージェント] > [エージェント管理] に移動します。
3. エージェントツリーで、バージョンアップするエージェントを選択します。1 つまたは複数のドメインを選択するか、ドメイン内のすべてまたは個別のエージェントを選択できます。
4. [設定] > [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
5. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。

6. [保存] をクリックします。
7. バージョンアップの結果をチェックします。
   - 87 ページの「オンラインエージェント」
   - 88 ページの「オフラインエージェント」
   - 89 ページの「スタンドアロンエージェント」
8. エージェントエンドポイントを再起動して、エージェントのバージョンアップを終了します。
9. 手順 2～8 を繰り返して、すべてのエージェントをバージョンアップします。

バージョンアップ結果

オンラインエージェント

注意

バージョンアップ後にエージェントエンドポイントを再起動します。

- 自動バージョンアップ

  次のいずれかのイベントが発生すると、オンラインエージェントのバージョンアップが開始されます。

  - Apex One サーバが新しいコンポーネントをダウンロードし、エージェントにアップデートするように通知したとき
  - エージェントが再ロードされたとき
  - エージェントが再起動し、Apex One サーバに接続したとき
  - エージェントエンドポイントで予約アップデートが実行されたとき (予約アップデートの権限があるエージェントのみ)
- 手動バージョンアップ

上記のいずれのイベントも発生しない場合、エージェントをただちにバージョンアップするには次のいずれかのタスクを実行します。

- セキュリティエージェントの EXE パッケージまたは MSI パッケージを作成して配信します。

  注意

  エージェントパッケージの作成手順については、管理者ガイドを参照してください。

- エージェントエンドポイントで [アップデート] を実行するようにユーザに指示します。
- `AutoPcc.exe` を右クリックして、[管理者として実行] を選択します。
- エージェントの手動バージョンアップを開始します。

手動バージョンアップを開始するには、次の手順を実行します。

1. [アップデート] > [エージェント] > [手動アップデート] に移動します。
2. [エージェントを手動で選択] オプションを選択し、[選択] をクリックします。
3. 表示されたエージェントツリーで、バージョンアップするエージェントを選択します。
4. エージェントツリーの上部にある [コンポーネントアップデートの開始] をクリックします。

オフラインエージェント

オフラインエージェントは、オンラインになったときにバージョンアップされます。

スタンドアロンエージェント

スタンドアロンモードのエージェントは、オンラインになったときにバージョンアップされるか、エージェントにバージョンアップ権限がある場合には、予約アップデートの実行時にバージョンアップされます。

バージョンアップ方法 3: Apex One Service Pack 1 サーバへのエージェントの移動

Apex One Service Pack 1 サーバの新規インストールを実行し、次にエージェントをこのサーバに移動します。エージェントを移動すると、自動的に Apex One Service Pack 1 にバージョンアップされます。

パート 1: Apex One サーバの新規インストールの実行とそれに続くアップデートの設定

手順

1. Apex One Service Pack 1 サーバの新規インストールを実行します。

   詳細については、54 ページの「セットアッププログラム」を参照してください。

2. Web コンソールにログオンします。

3. [アップデート] > [エージェント] > [自動アップデート] に移動し、次のオプションが有効であることを確認します。

   - Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する
   - 再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)

4. [エージェント] > [エージェント管理] に移動します。

5. エージェントツリーで、ルートドメインアイコン () をクリックしてすべてのエージェントを選択します。

6. [設定] > [権限とその他の設定] の順にクリックして、[その他の設定] タブに進みます。
7. [セキュリティエージェントがアップデートするコンポーネント] リストで、[すべてのコンポーネント (HotFix とエージェントプログラムを含む)] を選択します。
8. [すべてのエージェントに適用] をクリックします。
9. 以下の Apex One Service Pack 1 サーバの情報を記録します。エージェントの移動時に、前バージョンの Apex One サーバで以下の情報を指定します。
   - エンドポイント名または IP アドレス
   - サーバ待機ポート

     サーバ待機ポートを表示するには、[管理] > [設定] > [エージェント接続] に進みます。ポート番号が画面に表示されます。

パート 2: セキュリティエージェントのバージョンアップ

手順

1. 以前のサーバの Web コンソールで、[アップデート] > [概要] に移動します。
2. [通知のキャンセル] をクリックします。この機能では、サーバの通知キューをクリアして、Apex One サーバへのクライアント/エージェントの移動時の問題を防止します。

   警告!

   以降の手順もすぐに実行してください。クライアント/エージェントを移動する前にサーバ通知キューが更新された場合、クライアント/エージェントを正常に移動できない場合があります。
3. [エージェント] > [エージェント管理] に移動します。

4. エージェントツリーで、バージョンアップするエージェントを選択します。オフラインエージェントとスタンドアロンモードのエージェントは移動できないため、オンラインエージェントのみを選択してください。
5. 次の手順に従ってエージェントを移動します。
   a. [エージェントツリーの管理] > [エージェントの移動] の順にクリックします。
   b. [選択したエージェントを別の Apex One サーバに移動する] で、Apex One サーバのコンピュータ名/IP アドレスおよびサーバの待機ポートを指定します。
6. [移動] をクリックします。

バージョンアップ結果

- オンラインエージェントの移動とバージョンアップが開始されます。
- オフラインエージェントおよびスタンドアロンエージェントの管理についてのヒントを次に示します。
  - エージェントをバージョンアップするにはスタンドアロンモードを無効にします。
  - オフラインエージェントのユーザに、ネットワークに接続してエージェントをオンラインにするように指示します。長期間オフラインになっているエージェントについては、エンドポイントからアンインストールし、管理者ガイドで説明されている適切なエージェントインストール方法 (エージェントパッケージャなど) を使用して、セキュリティエージェントをインストールするようにユーザに指示してください。

注意

エージェントエンドポイントを再起動して、エージェントのバージョンアップを終了します。

バージョンアップ方法 4: エージェントの自動バージョンアップの有効化

Apex One サーバをこのバージョンにバージョンアップすると、サーバが管理するすべてのエージェントにバージョンアップするよう通知が送信されます。

サーバが管理するエージェントが少数の場合、エージェントに自動バージョンアップを許可することを検討してください。前述のバージョンアップ方法を使用することもできます。

パート 1: Apex One サーバでのアップデート設定

手順

1. [アップデート] > [エージェント] > [自動アップデート] に移動し、次のオプションが有効であることを確認します。
   - Apex One サーバが新しいコンポーネントをダウンロード後、ただちにエージェントのコンポーネントのアップデートを開始する
   - 再起動時、または Apex One サーバへの接続時にコンポーネントアップデートの開始を許可する (スタンドアロンモードのエージェントを除く)
2. [エージェント] > [エージェント管理] に移動します。
3. エージェントツリーで、ルートドメインアイコン ( ) をクリックしてすべてのエージェントを選択します。
4. [設定] > [権限とその他の設定] の順にクリックし、[その他の設定] タブに移動します。
5. [セキュリティエージェントがアップデートするコンポーネント] リストで、[パターンファイル] を選択します。
6. [すべてのエージェントに適用] をクリックします。

   ネットワーク環境が複雑な場合や、エージェント数が多い場合は、設定をオンラインエージェントに配信するのに時間がかかる場合がありま

す。バージョンアップ前に、設定をすべてのエージェントに配信するのに十分な時間を割り当ててください。設定を適用していないセキュリティエージェントは自動的にバージョンアップされます。

パート 2: Apex One サーバのバージョンアップ

Apex One サーバのバージョンアップの詳細については、94 ページの「ローカルバージョンアップの実行」を参照してください。

注意

バージョンアッププロセスの高速化を図るには、Windows Server 2008 Standard 64 ビット版を実行する Apex One サーバをバージョンアップする前に、セキュリティエージェントをアンロードします。

インストールの完了後、エージェントをバージョンアップする前に、Web コンソールを使用して Apex One サーバを設定します。

Apex One の詳細な設定手順については、管理者ガイドまたはサーバのオンラインヘルプを参照してください。

バージョンアップ結果

- オンラインエージェントは、サーバのバージョンアップが完了するとただちにバージョンアップされます。
- オフラインエージェントは、オンラインになったときにバージョンアップされます。
- スタンドアロンモードエージェントは、オンラインになったときにバージョンアップされるか、エージェントにバージョンアップ権限がある場合には、予約アップデートの実行時にバージョンアップされます。

注意

エージェントエンドポイントを再起動して、エージェントのバージョンアップを終了します。

ローカルバージョンアップの実行

ローカルバージョンアップでは、元の Apex One サーババージョンで使用されていた設定が適用され、Apex One Service Pack 1 の新機能に関連する設定画面だけが表示されます。

重要

データの損失に備え、Apex One サーバのバージョンアップ前に、以下のフォレンジックスフォルダとデータベースのバックアップを作成してください。

- <Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicData
- <Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicDataTracker.db

以下のファイルの場所を記録します。バージョンアッププロセスが完了したら、フォレンジックスフォルダとデータベースを元の場所に復元します。

使用許諾契約書

インストールを続行するには使用許諾契約をお読みいただき、使用許諾契約の条項に同意いただく必要があります。使用許諾契約の条項に同意いただけない場合には、インストールを続行することはできません。

フォレンジックスデータ

データの損失に備え、Apex One サーバで以下のフォレンジックスフォルダとデータベースのバックアップを手動で作成してください。

- <Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicData
- <Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥DLPForensicDataTracker.db

重要

以下のファイルの場所を記録します。バージョンアッププロセスが完了したら、フォレンジックスフォルダとデータベースを元の場所に復元します。

セキュリティエージェントのバージョンアップ

セットアッププログラムで対象エンドポイントのリソースが評価され、バージョンアップの場合に対象エンドポイントに以前のバージョンのセキュリティエージェントプログラムがあると、警告画面が表示されます。

拡張保護を有効にする

日本では提供していません。

データベースバックアップ

セットアッププログラムには、バージョンアップ時に、最新バージョンの Apex One へのバージョンアップ前に Apex One データベースをバックアップするオプションが用意されています。作成したバックアップ情報はロールバックの際に使用できます。

注意

バックアップパッケージには、300MB を超える空きディスク容量が必要になることがあります。

Endpoint Sensor のインストール

Apex Central と統合する場合で、Endpoint Sensor ライセンスの購入が済んでいるときは、[Endpoint Sensor のインストール] を選択してセキュリティエージェントで必要な Endpoint Sensor サービスがすべて利用できることを確認します。

注意

この機能が公式にサポートされているのは次のプラットフォームのみです。

- Windows 7 SP1
- Windows 8.1
- Windows10

次の表では、Endpoint Sensor サービスのインストールに必要な最小要件を示しています。

項目	要件	確認
Redis サービス	Apex One サーバコンピュータには、既存の Redis サービスをインストールできません。既存の Redis サービスをアンインストールしてから、セットアッププログラムを使用して新しいサービスをインストールする必要があります。	[Endpoint Sensor のインストール] 画面で [次へ] をクリックした後
SQL Server のバージョン	• SQL Server 2017 • SQL Server 2016 SP1 **注意** この機能では、SQL Server Express のバージョンはサポートされていません。	[Apex One データベースセットアップ] 画面で [次へ] をクリックした後
データベース設定	[検索のためのフルテキスト抽出とセマンティック抽出] を有効にする [検索のためのフルテキスト抽出とセマンティック抽出] の有効化の詳細については、SQL Server のドキュメントを参照してください。	[Apex One データベースセットアップ] 画面で [次へ] をクリックした後
	データベースメンテナンス機能を使用するための tempdb データベースへのアクセス権	なし

注意

Endpoint Sensor サービスをインストールしなかった場合や、[検索のためのフルテキスト抽出とセマンティック抽出] が有効になっているサポート対象のバージョンの SQL Server を選択しなかった場合に、Endpoint Sensor を後で使用するには、Windows の [コントロール パネル] にある [プログラムのアンインストールまたは変更] にアクセスする必要があります。

Apex One サーバを選択して、[変更] をクリックします。

Apex One データベースセットアップ

重要

Endpoint Sensor 機能の使用を検討している場合は、適切に準備された、サポートされているバージョンの SQL Server 上のデータベースを選択する必要があります。

詳細については、29 ページの「Apex One Endpoint Sensor」を参照してください。

手順

1. [SQL Server] に、Apex One で使用する既存の SQL Server とデータベースインスタンスを選択します。
2. データベースの認証方法を選択します。

   Windows アカウントを使用してサーバにログオンするときは、Apex One に現在ログオンしているユーザのユーザ名が適用されます。

   domain_name\user_name または user_name

重要

ユーザアカウントは、ローカル管理者グループに属しているか、Active Directory (AD) ビルトイン管理者である必要があります。また、Windows のローカルセキュリティポリシーまたはグループポリシー管理コンソールを使用して、次のユーザ権限割り当てポリシーを設定する必要があります。

- サービスとしてログオン
- バッチジョブとしてログオン
- ローカルログオンを許可

ユーザアカウントには、次に示すデータベースの役割も必要です。

- dbcreator
- bulkadmin
- db_owner

3. SQL Server 上の Apex One データベース名を指定します。
4. [次へ] をクリックします。

重要

Endpoint Sensor サービスのインストールを選択した場合は、セットアッププログラムにより、選択した SQL Server データベースが正しく設定され、最小要件を満たしているかどうかがただちに評価されます。SQL Server データベースが要件を満たしていない場合は、別の SQL Server データベースを選択するか、戻って Endpoint Sensor をインストールしない旨の選択をする必要があります。

Apex One セキュリティエージェント配信

セキュリティエージェントのインストールやバージョンアップは、複数の方法で行うことができます。この画面には、各種の配信方法と、必要なネットワーク帯域幅の概算値が表示されます。

この画面を使用して、セキュリティエージェントを対象エンドポイントに配信するときにサーバに必要な容量や、消費される帯域幅を確認します。

注意

すべてのインストール方法で、対象エンドポイントのローカル管理者権限またはドメイン管理者権限が必要になります。

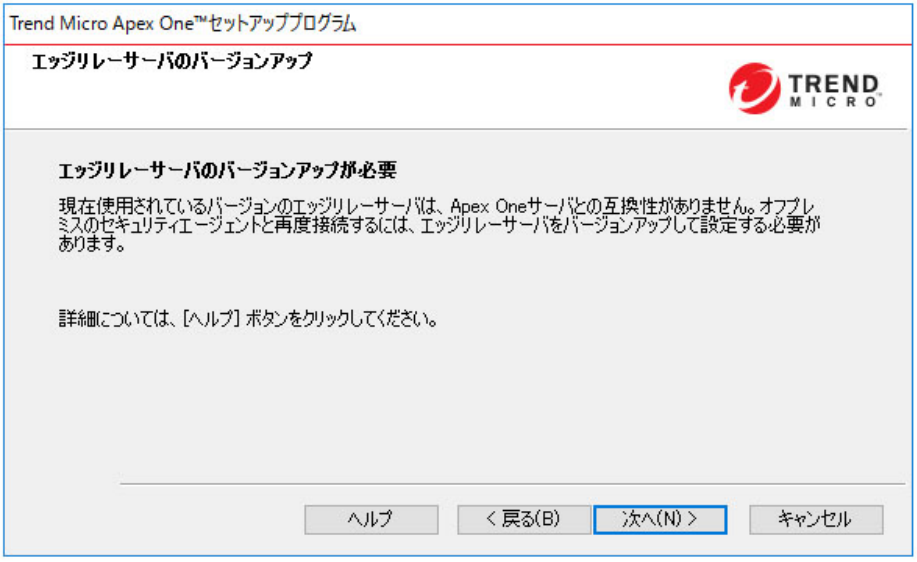
インストール情報

この画面は、インストール設定の概要を表示します。インストール情報が正しいことを確認し、[戻る] をクリックして設定やオプションを変更します。インストールを開始するには、[インストール] をクリックします。

エッジリレーサーバのアップデート

重要

以前の Apex One サーバにエッジリレーサーバを登録済みである場合にのみ表示されます。



Apex One では、旧ウイルスバスター Corp.のエッジリレーサーバをサポートしていません。オフプレミスのセキュリティエージェントを保護するには、新しいエッジリレーサーバをインストールするか、既存のエッジリレーサーバをバージョンアップする必要があります。

エッジリレーサーバのインストール後またはバージョンアップ後、エッジリレーサーバを使用して管理するすべてのセキュリティエージェントが ApexOne サーバに直接接続して最新のエッジリレーサーバ設定を取得する必要があります。

エッジリレーサーバのインストールまたはアップグレードの詳細については、Apex One 管理者ガイドを参照してください。

InstallShield Wizard の完了

インストールが完了したら、製品の基本情報や既知の問題などが記載された Readme ファイルを確認してください。

以下の場所に、バックアップしたフォレンジックスフォルダとデータベースを復元します。

```
<Apex One サーバのインストールフォルダ>¥PCCSRV¥Private¥
```

管理者は、Web コンソールを起動して、Apex One の設定を開始できます。

第 4 章

インストール後のタスク

Apex One サーバのインストールが完了したら、次のタスクを実行します。

この章の内容

サーバのインストールまたはバージョンアップの確認

インストールまたはバージョンアップの完了後に、以下のことを確認してください。

表 4-1. Apex One インストール後の確認事項

確認事項	詳細
Apex One サーバのショートカット	サーバコンピュータの Windows の [スタート] メニューに、Apex One サーバのショートカットがあること。
プログラムリスト	サーバコンピュータのコントロールパネルの [プログラムの追加と削除] リストに Apex One サーバが含まれていること。
Apex One Web コンソール	Internet Explorer ブラウザに次の URL を入力する。 • HTTPS 接続: `https://<Apex One サーバ名>:<ポート番号>/officescan` <Apex One サーバ名>は、Apex One サーバの名前または IP アドレスです。 Web コンソールのログオン画面が表示されます。

確認事項	詳細
Apex One サーバサービス	Microsoft 管理コンソールに次の Apex One サーバサービスが表示されていること。 • Apex One Active Directory Integration Service: Active Directory 統合と役割ベースの管理機能が正常に稼働している場合、このサービスが表示されます。 • Apex One Apex Central Agent: Apex One サーバが Apex Central に登録されている場合、このサービスのステータスは「開始済み」になっている必要があります。 • Apex One Deep Discovery Service: このサービスのステータスは「開始済み」になっている必要があります。 • Apex One Master Service: このサービスのステータスは「開始済み」になっている必要があります。 • Apex One Log Receiver Service: このサービスのステータスは「開始済み」になっている必要があります。 • Apex One Plug-in Manager: このサービスのステータスは「開始済み」になっている必要があります。 • Trend Micro Smart Protection Query Handler: このサービスのステータスは「開始済み」になっている必要があります。 • Trend Micro Smart Protection Server: このサービスのステータスは「開始済み」になっている必要があります。 • Trend Micro Local Web Classification Server:インストール時に Web レピュテーションサービスを有効にした場合、このサービスのステータスは「開始済み」になっている必要があります。
Apex One サーバのプロセス	Windows タスクマネージャを開いたとき、DBServer.exe が実行されていること。
サーバのインストールログ	サーバインストールログ OFCMAS.LOG が、`%windir%`にあること。

確認事項	詳細
レジストリキー	次のレジストリキーが存在すること。 • 32 ビットプラットフォームの場合: HKEY_LOCAL_MACHINE¥Software¥TrendMicro¥OfficeScan • 64 ビットプラットフォームの場合: HKEY_LOCAL_MACHINE¥Software¥Wow6432Node¥TrendMicro¥OfficeScan
プログラムフォルダ	Apex One サーバファイルが<サーバインストールフォルダ>にあること。

統合 Smart Protection Server のインストールの確認

新規インストール時に、Apex One によって自動的に統合 Smart Protection Server がインストールされます。

手順

1. サーバの Web コンソールで、[管理] > [Smart Protection] > [Smart Protection ソース] に移動します。
2. [標準リスト] リンクをクリックします。
3. 表示される画面で、[統合 Smart Protection Server] をクリックします。
4. 表示される画面で、[接続テスト] をクリックします。

   統合サーバとの接続が正常に行われる必要があります。

Apex One サーバのアップデート

Apex One のインストール後、サーバのコンポーネントをアップデートしてください。

注意

このセクションでは手動アップデートの方法を紹介します。予約アップデートまたはアップデート設定については、サーバのオンラインヘルプを参照してください。

手順

1. Web コンソールにログオンします。
2. メインメニューで、[アップデート] > [サーバ] > [手動アップデート] の順にクリックします。

   [手動アップデート] 画面に、現在のコンポーネントとそのバージョン番号、および最終アップデート日時が表示されます。
3. アップデート対象コンポーネントを選択します。
4. [アップデート] をクリックします。アップデートサーバに新しいコンポーネントがあるかどうかが確認されます。アップデートが進行し、ステータスが表示されます。

初期設定の確認

Apex One は初期設定でインストールされます。これらの設定がセキュリティ要件に適合していない場合は、Web コンソールで設定を変更します。Web コンソールで可能な設定の詳細については、サーバのオンラインヘルプと管理者ガイドを参照してください。

検索設定

Apex One は、エンドポイントをセキュリティリスクから保護するために複数の検索方法を提供します。検索設定を変更するには、Web コンソールで [エージェント] > [エージェント管理] に移動し、[設定] > {検索の種類} の順にクリックします。

エージェント設定

Apex One には、サーバに登録されたすべてのエージェント、または特定の権限を持つすべてのエージェントに適用される設定が何種類かあります。エージェント設定を変更するには、Web コンソールで [エージェント] > [グローバルエージェント設定] に移動します。

エージェント権限

初期設定のエージェント権限には、セキュリティエージェントエンドポイントのシステムトレイアイコンの表示が含まれます。初期設定のエージェント権限は Web コンソールで変更できます。

1. [エージェント] > [エージェント管理] に移動します。
2. [設定] > [権限とその他の設定] の順にクリックします。

Apex One の Apex Central への登録

新しくインストールした Apex One サーバを Apex Central サーバで管理する場合、インストール後、Apex Central に Apex One を登録します。

注意

Apex Central への登録が必要なのは、新しくインストールされた Apex One サーバのみです。

Apex One Web コンソールで、[管理] > [設定] > [Apex Central] に移動します。

手順については、Apex One サーバのヘルプまたは Apex One の管理者ガイドを参照してください。

第 5 章

Apex One のアンインストール

この章では、Apex One サーバをアンインストールする手順について説明します。

この章の内容

アンインストールの注意事項

Apex One で問題が発生したときは、アンインストールプログラムを使用して、エンドポイントから Apex One サーバを安全に削除します。サーバをアンインストールする前に、そのサーバが管理するエージェントを別の Apex One サーバに移動してください。

Apex One サーバをアンインストールする前の作業

アンインストールプログラムを使用して、Apex One サーバを安全に削除します。

サーバをアンインストールする前に、そのサーバが管理するエージェントを同じバージョンの別の Apex One サーバに移動してください。サーバを後から再インストールする場合は、サーバデータベースと設定ファイルをバックアップすることを検討してください。

別のサーバへのエージェントの移動

Apex One Web コンソールには、サーバで管理されているエージェントを別のサーバへ移動するオプションがあります。

手順

1. 移動先のサーバに関する次の情報をメモに記録します。この情報は、エージェントを移動するときに必要になります。

   - エンドポイント名または IP アドレス
   - サーバ待機ポート

   サーバ待機ポートを表示するには、[管理] > [設定] > [エージェント接続] の順に進みます。ポート番号が画面に表示されます。

2. アンインストールするサーバの Web コンソールで、[エージェント] > [エージェント管理] の順に移動します。

3. エージェントツリーで、移動するエージェントを選択し、[エージェントツリーの管理] > [エージェントの移動]の順にクリックします。
4. [選択したエージェントを別の Apex One サーバに移動する] で、移動先の Apex One サーバのコンピュータ名/IP アドレスとサーバ待機ポートを指定します。
5. [移動] をクリックします。

すべてのエージェントが移動し、移動先のサーバで管理されていることを確認したら、Apex One サーバを安全にアンインストールできます。

Apex One 設定ファイルのバックアップと復元

Apex One サーバをアンインストールする前に、重要な設定ファイルをバックアップします。

注意

Apex One では、アンインストールプロセス中に SQL データベースを削除しないオプションが用意されています。

手順

1. Microsoft 管理コンソールから、Apex One Master Service を停止します。
2. <サーバのインストールフォルダ>¥PCCSRV フォルダにある次のファイルとフォルダを手動でバックアップします。
   - ofcscan.ini:グローバルエージェント設定が含まれます。
   - ous.ini:ウイルス対策コンポーネント配信用のアップデート元情報が含まれます。
   - Private フォルダ: ファイアウォールとアップデート元設定が含まれます。
   - Web¥tmOPP フォルダ: 大規模感染予防設定が含まれます。
   - Pccnt¥Common¥OfcPfw*.dat:ファイアウォール設定が含まれます。

- `Download¥OfcPfw*.dat`: ファイアウォール配信設定が含まれます。
- Log フォルダ: システムイベントおよび接続状態の確認ログが含まれます。
- Virus フォルダ: 隔離されたファイルが含まれます。

3. Apex One サーバをアンインストールします。

   詳細については、110 ページの「Apex One サーバのアンインストール」を参照してください。

4. 新規インストールを実行します。

   詳細については、54 ページの「セットアッププログラム」を参照してください。

5. セットアップの終了後、Microsoft 管理コンソール (`services.msc`) を開きます。

6. [Apex One Master Service] を右クリックし、[停止] をクリックします。

7. 対象エンドポイントの<サーバのインストールフォルダ>¥PCCSRV フォルダにバックアップファイルをコピーします。

8. Apex One Master Service を再起動します。

Apex One サーバのアンインストール

アンインストールプログラムを使用して、Apex One サーバおよび統合 Smart Protection Server をアンインストールします。

アンインストールプログラムで問題が発生した場合には、手動でサーバをアンインストールします。

注意

セキュリティエージェントのアンインストール手順については、管理者ガイドを参照してください。

アンインストールプログラムによる Apex One サーバのアンインストール

手順

1. アンインストールプログラムを実行します。アンインストールプログラムには、次の 2 種類の方法でアクセスできます。

   - 方法 A

     a. Apex One サーバコンピュータで、[スタート] > [プログラム] > [Trend Micro Apex One サーバ] > [Apex One のアンインストール] の順にクリックします。確認画面が表示されます。

     b. [はい] をクリックします。サーバのアンインストールプログラムでは、管理者パスワードが求められます。

     c. 管理者パスワードを入力し、[OK] をクリックします。サーバのアンインストールプログラムがサーバファイルの削除を開始します。確認のメッセージが表示されます。

     d. [OK] をクリックしてアンインストールプログラムを閉じます。

   - 方法 B

     a. Windows の [プログラムの追加と削除] 画面で、Apex One サーバプログラムをダブルクリックします。

     b. [コントロール パネル] > [プログラムの追加と削除] の順にクリックします。[Trend Micro Apex One サーバ] を探してダブルクリックします。管理者パスワードが求められるまで、画面に表示される指示に従います。

     c. 管理者のパスワードを入力し、[OK] をクリックします。サーバのアンインストールプログラムによるサーバファイルの削除が開始されます。確認メッセージが表示されます。

     d. [OK] をクリックしてアンインストールプログラムを閉じます。

Apex One サーバの手動アンインストール

パート 1: 統合 Smart Protection Server のアンインストール

手順

1. Microsoft 管理コンソール (MMC) を開き、Apex One Master Service を停止します。
2. コマンドプロンプトを開いて、<サーバのインストールフォルダ>¥PCCSRV に進みます。
3. 次のコマンドを実行します。

   ```
   SVRSVCSETUP.EXE -uninstall
   ```

   このコマンドは Apex One 関連のサービスをアンインストールしますが、設定ファイルや Apex One データベースは削除されません。
4. <サーバのインストールフォルダ>¥PCCSRV¥private に移動し、ofcserver.ini を開きます。
5. 次の設定を変更します。

   表 5-1. ofcserver.ini の設定

設定	手順
WSS_INSTALL=1	1 を 0 に変更
WSS_ENABLE=1	この行を削除
WSS_URL=https://<コンピュータ名>:4345/tmcss/	この行を削除

6. <サーバのインストールフォルダ>¥PCCSRV に移動し、OfUninst.ini を開きます。次の行を削除します。

   ```
   [WSS_WEB_SERVER]

   ServerPort=8082

   IIS_VhostName=Smart Protection Server (Integrated)
   ```

```
IIS_VHostIdx=5
```

注意

IIS_VHostidx の値は、次の行の「isapi」値と同じでなければなりません。

```
ROOT=/tmcss,C:\Program Files\Trend
Micro\OfficeScan\PCCSRV\WSS\isapi,,<値>
```

```
[WSS_SSL]

SSLPort=<SSL ポート>
```

7. コマンドプロンプトを開いて、<サーバのインストールフォルダ>¥PCCSRV に進みます。
8. 次のコマンドを実行します。

```
Svrsvcsetup -install

Svrsvcsetup -enablessl

Svrsvcsetup -setprivilege
```

9. 次の項目が削除されていることを確認します。
   - Microsoft 管理コンソールの Trend Micro Smart Protection Server service
   - Smart Protection Server のパフォーマンスカウンタ
   - Smart Protection Server (統合) Web サイト

パート 2: Apex One サーバのアンインストール

手順

1. レジストリエディタを開いて、次の手順を実行します。

警告!

次の手順ではレジストリキーの削除が必要です。レジストリキーを誤って変更すると、システムに重大な問題が生じる可能性があります。レジストリキーを変更する場合は必ずバックアップコピーを作成してください。詳細については、レジストリエディタのヘルプを参照してください。

a. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\に移動します。

b. ofcservice が削除されていることを確認します。

c. HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\OfficeScan\に移動し、OfficeScan を削除します。

64 ビットエンドポイントの場合、パスは HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Trend Micro\OfficeScan\です。

d. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\に移動し、OfficeScan Management Console-<サーバ名>フォルダを削除します。

2. <サーバのインストールフォルダ>¥PCCSRV フォルダに移動し、PCCSRV フォルダの共有を解除します。

3. サーバコンピュータを再起動します。

4. <サーバのインストールフォルダ>¥PCCSRV に移動し、PCCSRV フォルダを削除します。

5. インターネットインフォメーションサービス (IIS) コンソールで、Apex One の Web サイトを削除します。

a. IIS コンソールを開きます。

b. サーバ名を展開します。

c. Apex One を別の Web サイトにインストールしている場合は、[Web サイト] フォルダに進み、Apex One を削除します。

d. Apex One の仮想ディレクトリを既定の Web サイトにインストールしている場合は、[既定の Web サイト] に進み、Apex One の仮想ディレクトリを削除します。

第 6 章

トラブルシューティングのリソース

この章では、このバージョンの Apex One で発生した問題のトラブルシューティングに役立つリソースについて説明します。

この章は次のトピックで構成されます。

サポートインテリジェンスシステム

サポートインテリジェンスシステムのページを使用すると、分析用のファイルをトレンドマイクロに簡単に送信できます。このシステムでは、Apex One サーバの GUID が特定され、分析ファイルとともに送信されます。GUID は、トレンドマイクロが診断のために送られてきたファイルに関するフィードバックを提供する手助けとなります。

ケース診断ツール

トレンドマイクロのケース診断ツール (cdt) は、問題が発生した場合にお客様の製品から必要なデバッグ情報を収集します。そして、製品のデバッグステータスをオンまたはオフに自動的に切り替えて、問題のカテゴリに従って必要なファイルを収集します。トレンドマイクロはこの情報を使用して、製品に関連する問題をトラブルシューティングします。

このツールと関連マニュアルの入手については、サポート担当者にお問い合わせください。

Trend Micro パフォーマンス調整ツール

トレンドマイクロでは、潜在的にパフォーマンスの問題を引き起こす可能性があるアプリケーションを特定する、スタンドアロンのパフォーマンス調整ツールを用意しています。Trend Micro パフォーマンス調整ツールは、テストインストール時にスタンドアロンのワークステーションのイメージや少数のインストール先ワークステーションで実行し、挙動監視およびデバイスコントロールを実際にインストールする前に、パフォーマンスの問題を解決します。

システム負荷の高いアプリケーションの特定

Trend Micro パフォーマンス調整ツールについては、次を参照してください。

https://success.trendmicro.com/jp/solution/1310435

インストールログ

Apex One では、インストールの問題の解決に役立つインストールログファイルが自動的に生成されます。

表 6-1. インストールログファイル

ログファイル	ファイル名	場所
サーバのローカルインストール/バージョンアップログ	OFCMAS.LOG	%windir%
サーバのリモートインストール/バージョンアップログ	OFCMAS.LOG (セットアップを起動したエンドポイント上) OFCMAS.LOG (対象エンドポイント上)	%windir%
セキュリティエージェントインストールログ	OFCNT.LOG	MSI パッケージ以外のすべてのインストール方法は%windir% MSI パッケージのインストール方法は%temp%

サーバのデバッグログ

次のサーバタスクを実行する前に、デバッグログを有効にします。

- サーバをアンインストールして、再度インストールします。
- Apex One を新しいバージョンにバージョンアップする。
- リモートインストール/バージョンアップを実行する (デバッグログはセットアップを起動したエンドポイントでのみ有効となり、リモートエンドポイントには適用されません)。

警告!

デバッグログはサーバの性能に影響を与え、大量のディスク空き容量を消費する可能性があります。必要なときにのみデバッグログを有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

Apex One サーバコンピュータでのデバッグログの有効化

オプション 1:

手順

1. Web コンソールにログオンします。
2. Web コンソールのバナーで、「Apex」の [A] をクリックします。[デバッグログ設定] 画面が開きます。
3. デバッグログ設定を指定します。
4. [保存] をクリックします。
5. 次の初期設定の場所にあるログファイル (ofcdebug.log) をチェックします。<サーバのインストールフォルダ>¥PCCSRV¥Log

オプション 2:

手順

1. <サーバのインストールフォルダ>¥PCCSRV¥Private にある「LogServer」フォルダを C:¥にコピーします。
2. ofcdebug.ini という名前のファイルを作成し、次の内容を入力します。

```
[debug]

DebugLevel=9

DebugLog=C:¥LogServer¥ofcdebug.log
```

```
debugLevel_new=D

debugSplitSize=10485760

debugSplitPeriod=12

debugRemoveAfterSplit=1
```

3. ofcdebug.ini を C:¥LogServer に保存します。
4. 適切なタスクを実行します (サーバの再インストール、新しいサーババージョンへのバージョンアップ、またはリモートでのインストール/バージョンアップ)。
5. C:¥LogServer の ofcdebug.log を確認します。

注意

Apex One サーバにセキュリティエージェントがある場合、エージェントのデバッグログもサーバのデバッグログに出力されます。

エージェントのデバッグログ

セキュリティエージェントをインストールする前に、デバッグログを有効にします。

警告!

デバッグログはエージェントパフォーマンスに影響し、大量のディスク空き容量を消費する可能性があります。必要なときにのみデバッグログを有効にし、デバッグデータが不要になった場合はただちに無効にしてください。ファイルサイズが巨大になった場合はログファイルを削除してください。

セキュリティエージェントでのデバッグログの有効化

手順

1. ofcdebug.ini という名前のファイルを作成し、次の内容を入力します。

   ```
   [Debug]

   Debuglog=C:¥ofcdebug.log

   debuglevel=9

   debugLevel_new=D

   debugSplitSize=10485760

   debugSplitPeriod=12

   debugRemoveAfterSplit=1
   ```

2. ofcdebug.ini ファイルをエージェントユーザに送信し、C:¥フォルダ内に保存するように指示します。

   LogServer.exe は、エージェントエンドポイントが起動するたびに自動的に起動します。

3. デバッグログを開始するには、セキュリティエージェントを再ロードするか、エンドポイントを再起動します。

   エンドポイントの起動時に LogServer.exe コマンドウィンドウが開き、Apex One に対してデバッグログ生成の中止を要求しますが、ユーザに対してこのウィンドウを閉じないように指示してください。ユーザがコマンドウィンドウを閉じた場合には、¥Security Agent¥Temp 内にある LogServer.exe を起動すると再度デバッグログ生成を開始できます。

4. それぞれのエージェントエンドポイントについて、C:¥内の ofcdebug.log を確認します。

5. セキュリティエージェントのデバッグログを無効にするには、ofcdebug.ini ファイルを削除します。

第 7 章

テクニカルサポート

ここでは、次の項目について説明します。

トラブルシューティングのリソース

トレンドマイクロでは以下のオンラインリソースを提供しています。テクニカルサポートに問い合わせる前に、こちらのサイトも参考にしてください。

サポートポータルの利用

サポートポータルでは、よく寄せられるお問い合わせや、障害発生時の参考となる情報、リリース後に更新された製品情報などを提供しています。

https://success.trendmicro.com/jp/technical-support

脅威データベース

現在、不正プログラムの多くは、コンピュータのセキュリティプロトコルを回避するために、2 つ以上の技術を組み合わせた複合型脅威で構成されています。トレンドマイクロは、カスタマイズされた防御戦略を策定した製品で、この複雑な不正プログラムに対抗します。脅威データベースは、既知の不正プログラム、スパム、悪意のある URL、および既知の脆弱性など、さまざまな混合型脅威の名前や兆候を包括的に提供します。

詳細については、https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/ をご覧ください。

- 現在アクティブまたは「in the Wild」と呼ばれている生きた不正プログラムと悪意のあるモバイルコード
- これまでの Web 攻撃の記録を記載した、相関性のある脅威の情報ページ
- 対象となる攻撃やセキュリティの脅威に関するオンライン勧告
- Web 攻撃およびオンラインのトレンド情報
- 不正プログラムの週次レポート

製品サポート情報

製品のユーザ登録により、さまざまなサポートサービスを受けることができます。

トレンドマイクロの Web サイトでは、ネットワークを脅かすウイルスやセキュリティに関する最新の情報を公開しています。ウイルスが検出された場合や、最新のウイルス情報を知りたい場合などにご利用ください。

サポートサービスについて

サポートサービス内容の詳細については、製品パッケージに同梱されている「製品サポートガイド」または「スタンダードサポートサービスメニュー」をご覧ください。

サポートサービス内容は、予告なく変更される場合があります。また、製品に関するお問い合わせについては、サポートセンターまでご相談ください。トレンドマイクロのサポートセンターへの連絡には、電話またはお問い合わせ Web フォームをご利用ください。サポートセンターの連絡先は、「製品サポートガイド」または「スタンダードサポートサービスメニュー」に記載されています。

サポート契約の有効期限は、ユーザ登録完了から 1 年間です (ライセンス形態によって異なる場合があります)。契約を更新しないと、パターンファイルや検索エンジンの更新などのサポートサービスが受けられなくなりますので、サポートサービス継続を希望される場合は契約満了前に必ず更新してください。更新手続きの詳細は、トレンドマイクロの営業部、または販売代理店までお問い合わせください。

注意

サポートセンターへの問い合わせ時に発生する通信料金は、お客さまの負担とさせていただきます。

トレンドマイクロへのウイルス解析依頼

ウイルス感染の疑いのあるファイルがあるのに、最新の検索エンジンおよびパターンファイルを使用してもウイルスを検出/ 駆除できない場合などに、感

染の疑いのあるファイルをトレンドマイクロのサポートセンターへ送信していただくことができます。

ファイルを送信いただく前に、トレンドマイクロの不正プログラム情報検索サイト「脅威データベース」にアクセスして、ウイルスを特定できる情報がないかどうか確認してください。

https://www.trendmicro.com/vinfo/jp/threat-encyclopedia/

ファイルを送信いただく場合は、次の URL にアクセスして、サポートセンターの受付フォームからファイルを送信してください。

https://success.trendmicro.com/jp/virus-and-threat-help

感染ファイルを送信する際には、感染症状について簡単に説明したメッセージを同時に送ってください。送信されたファイルがどのようなウイルスに感染しているかを、トレンドマイクロのウイルスエンジニアチームが解析し、回答をお送りします。

感染ファイルのウイルスを駆除するサービスではありません。ウイルスが検出された場合は、ご購入いただいた製品にてウイルス駆除を実行してください。

メールレピュテーションについて

スパムメールやフィッシングメールなどの送信元を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

ファイルレピュテーションについて

不正プログラムなどのファイル情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

Web レピュテーションについて

不正な Web サイトや URL などの情報を、脅威情報のデータベースと照合することによって判別して評価する、トレンドマイクロのコアテクノロジーです。コアテクノロジーの詳細については、次の Web ページを参照してください。

https://www.trendmicro.com/ja_jp/business/technologies/smart-protection-network.html

その他のリソース

製品やサービスについてのその他の情報として、次のようなものがあります。

最新版ダウンロード

製品やドキュメントの最新版は、次の Web ページからダウンロードできます。

https://downloadcenter.trendmicro.com/index.php?clk=left_nav&clkval=all_download&regs=jp

注意

サービス製品、販売代理店経由での販売製品、または異なる提供形態をとる製品など、一部対象外の製品があります。

脅威解析・サポートセンター TrendLabs (トレンドラボ)

TrendLabs (トレンドラボ) は、フィリピン・米国に本部を置き、日本・台湾・ドイツ・アイルランド・中国・フランス・イギリス・ブラジルの 10 カ国 12 か所の各国拠点と連携してソリューションを提供しています。

世界中から選び抜かれた 1,000 名以上のスタッフで 24 時間 365 日体制でインターネットの脅威動向を常時監視・分析しています。

付録 A

導入例

このセクションでは、ネットワークトポロジや使用可能なネットワークリソースに応じた、Apex One の導入方法を説明します。組織内で Apex One の導入を計画する際の参考にしてください。

基本的なネットワーク

図 1 は、Apex One サーバとエージェントが直接接続されている基本的なネットワークを表しています。多くのビジネスネットワークがこの構成で、LAN (または WAN) の接続速度は 10Mbps、100Mbps、または 1Gbps です。この構成では、Apex One のシステム要件を満たし、十分なリソースを備えたエンドポイントが、Apex One サーバをインストールする第一候補となります。

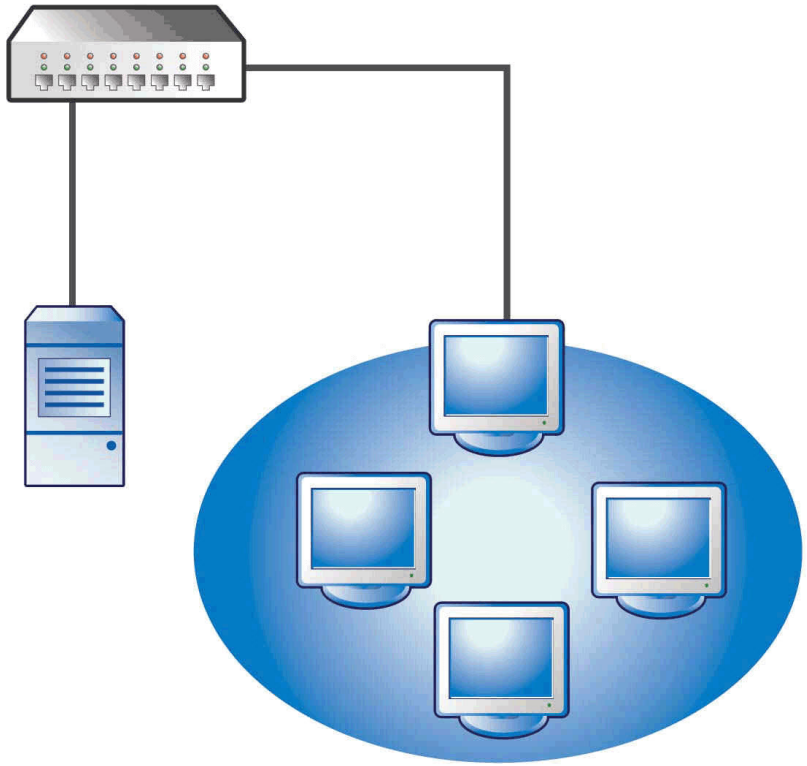


図 A-1. 基本的なネットワークトポロジ

複数サイトネットワーク

帯域幅の異なる複数のアクセスポイントやリモートサイトで構成されるネットワークについては、次の検討を行ってください。

- オフィスやネットワーク帯域幅の見地から統合ポイントを分析します。
- オフィスごとに現在の帯域幅利用率を判断します。

この情報を基に、Apex One の最適な配信方法を検討します。図 A-2 は、複数サイトのネットワークトポロジを表しています。

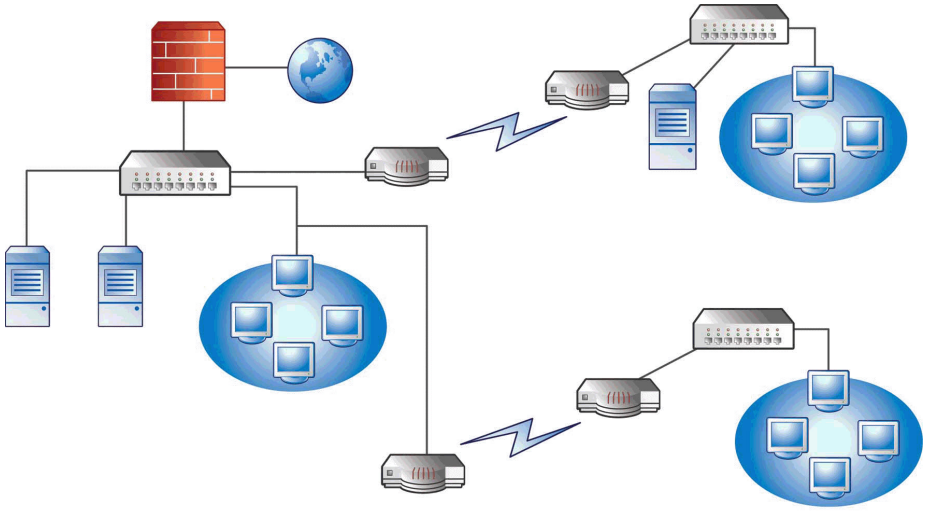


図 A-2. 複数サイトのネットワークトポロジ

ネットワーク情報:

- リモートサイト 1 の WAN リンクは業務時間中の平均利用が約 70%。このサイトには 35 台のエージェントエンドポイントがあります。
- リモートサイト 2 の WAN リンクは業務時間中の平均利用が約 40%。このサイトには 9 台のエージェントエンドポイントがあります。

- サーバ 3 は、リモートサイト 1 のグループのファイルおよびプリントサーバとしてのみ使用されています。このエンドポイントに Apex One サーバをインストールすることも検討できますが、追加の管理オーバーヘッドと引き換えにするほどの価値はないかもしれません。サーバはすべて Windows Server 2012 を実行しています。ネットワークでは Active Directory を使用していますが、その用途は主にネットワーク認証です。
- ヘッドオフィス、リモートサイト 1、リモートサイト 2 のエージェントエンドポイントは、すべて Windows Server 2012 または Windows 7 を実行しています。

複数サイトネットワークの準備

手順

1. Apex One サーバをインストールするエンドポイントを特定します。
2. 使用可能なエージェントのインストール方法を特定し、要件を満たさない方法を除外します。エージェントのインストール方法の詳細については、管理者ガイドを参照してください。

   使用可能なインストール方法

   - ログオンスクリプトウィザード

     ローカルトラフィックに問題がないため WAN を設置していない場合は、ログオンスクリプトセットアップを使用するとよいでしょう。ただし、各エンドポイントに 50MB 以上のデータを転送する場合は、この方法は使用できません。

   - Web コンソールからのリモートインストール

     この方法はヘッドオフィスで LAN 接続されているすべてのエンドポイントに有効です。これらのエンドポイントはすべて Windows Server 2012 を実行しているため、エンドポイントへのパッケージ配信は簡単です。

     この 2 つのリモートサイトは低速でリンクされているため、業務時間中に Apex One を配信する場合は、使用可能な帯域幅に影響を与えるおそれがあります。ほとんどの社員がオフィスにいない業務時間

外であれば、全リンク容量を使用して Apex One を配信できます。ただし、ユーザがエンドポイントの電源を切っていると、Apex One を配信できません。

- セキュリティエージェントパッケージの配信

  リモートサイトへの配信については、セキュリティエージェントパッケージの配信が最も適していると思われます。ただし、リモートサイト 2 にはこの方法をに対応できるローカルサーバがありません。すべての方法を詳しく見てみると、大半のエンドポイントではこの方法が最適な方法です。

ヘッドオフィスの配信

ヘッドオフィスに適した最も簡単なエージェント配信方法は、Apex One Web コンソールからのリモートインストールです。手順については、管理者ガイドを参照してください。

リモートサイト 1 の配信

リモートサイト 1 への配信には、Microsoft の分散ファイルシステム (DFS) の設定が必要です。DFS の詳細については、http://support.microsoft.com/?kbid=241452 を参照してください。DFS の設定後に、リモートサイト 1 のサーバ 3 は、既存の DFS 環境を複製するか、新しい環境を作成して DFS を有効にする必要があります。

推奨される配信方法は、Microsoft Installer Package (MSI) 形式で作成したエージェントパッケージを DFS に配信する方法です。手順については、管理者ガイドを参照してください。エージェントパッケージは次回の予約アップデート時にサーバ 3 にコピーされるため、帯域幅への影響を最小限に抑えることができます。

エージェントパッケージは Active Directory を利用して配信することもできます。詳細については、管理者ガイドを参照してください。

コンポーネントアップデートが WAN に与える影響を最小限に抑える

手順

1. リモートサイト 1 のアップデートエージェントとして使用するエージェントを 1 つ指定します。
   a. Web コンソールにログオンし、[エージェント] > [エージェント管理] に移動します。
   b. エージェントツリーで、アップデートエージェントとして使用するエージェントを選択し、[設定] > [エージェントアップデート設定] の順にクリックします。
2. リモートサイト 1 のエージェントのうち、アップデートエージェントからコンポーネントをアップデートするエージェントを選択します。
   a. [アップデート] > [サーバ] > [アップデート元] に移動します。
   b. [ユーザ指定アップデート元] を選択して、[追加] をクリックします。
   c. 表示された画面で、リモートサイト 1 のエンドポイントの IP アドレス範囲を入力します。
   d. [アップデート元] をオンにし、ドロップダウンリストから指定されたアップデートエージェントを選択してください。

リモートサイト 2 の配信

リモートサイト 2 の問題は帯域幅の低さです。しかし、約 154K ビットの帯域幅が使用可能な業務時間中に帯域幅の 60%が空いています。

セキュリティエージェントをインストールする最良の方法は、リモートサイト 1 と同じ MSI 形式のエージェントパッケージを使用することです。ただし、使用できるサーバがないため、分散ファイルシステム (DFS) は使用できません。

代替策として、他社製の管理ツールを使用して、管理者がリモートエンドポイントに物理的にアクセスすることなく、エンドポイントに共有ディレクト

リを設定または作成します。1 台のエンドポイントに共有ディレクトリを作成し、エージェントパッケージをその共有ディレクトリにコピーすれば、9 台のエンドポイントにエージェントをインストールするよりもオーバーヘッドを抑えることができます。

別の Active Directory ポリシーを使用し、ただしその場合もソースとして DFS 共有は指定しません。

これらの方法は、インストールトラフィックをローカルネットワーク内にとどめ、WAN 内のトラフィックを最小限に抑えます。

コンポーネントアップデートが WAN に与える影響を最小限に抑えるため、アップデートエージェントとして使用するエージェントを 1 つ指定します。詳細については、133 ページの「リモートサイト 1 の配信」を参照してください。

索引